FFG
Forschung wirkt.

Bundesministerium
Finanzen

AUSSCHREIBUNG 2023
EINREICHFRIST: 01.03.2024, 12:00 UHR
EINREICHFRIST INNOVATION AKUT: 31.01.2024, 12:00 UHR

KIRAS/K-PASS AUSSCHREIBUNG 2023
AUSSCHREIBUNGSLEITFADEN

KIRAS Sicherheitsforschung
K-PASS

IMPRESSUM

Eigentümer, Herausgeber und Medieninhaber
Bundesministerium für Finanzen (BMF)
Johannesgasse 5, 1010 Wien

Programmverantwortung KIRAS/K-PASS
Bundesministerium für Finanzen (BMF)
Sektion VI - Telekommunikation, Post und Bergbau
Stabsstelle für Sicherheitsforschung und Technologietransfer
Radetzkystraße 2, 1030 Wien

Programmabwicklung
Österreichische Forschungsförderungsgesellschaft mbH (FFG)
Bereich Thematische Programme
Sensengasse 1, 1090 Wien

Wien, Oktober 2023

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS 8

1 DAS WICHTIGSTE IN KÜRZE 9

2 MOTIVATION 11

2.1 Hintergrund KIRAS 11

2.2 Hintergrund K-PASS 12

2.3 Zielgruppen und Förderwerber 13

2.4 Die Möglichkeit der Klassifizierung 14

3 AUSSCHREIBUNGSSCHWERPUNKTE 15

3.1 KIRAS. Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für kooperative F&E-Projekte 16

3.1.1 Innovative multimodale und multisensorale Monitoringlösungen durch UAVs mit alternativen Antriebssystemen 16

3.1.2 Kontaminationsmonitor - Feststellung von Kontaminationsrückständen mit optischen Detektionsmethoden 17

3.1.3 Technische Möglichkeiten zur Personalreduktion beim Schutz kritischer Infrastruktur 18

3.1.4 Erhebung und Berechnung von geologischen sowie geographischen Daten mittels der Kombination von Feldmethoden und der Geoanalyse von Satellitenbildern 19

3.1.5 Early Warning Tool für Lieferkettenunterbrechungen für Lebensmittel 20

3.1.6 Aufbau und Entwicklung einer innovativen Gebäudedatenbank zur Unterstützung der Analyse der physischen Verwundbarkeit von Gebäuden gegenüber Naturgefahren 21

3.1.7 Netzwerkmodellierungen zur systemischen Risikobewertung der Lieferkettenabhängigkeiten kritischer Güter 22

3.1.8 Erstellung eines umfassenden Versorgungslagebilds im Sinne der Versorgungssicherungsgesetze durch einen abgestimmt kontrollierten Zugriff auf interne Unternehmensdaten im Krisenfall 23

3.1.9 Intelligentes Meldungs- und Alarm-Management für Technisches Monitoring in kritischen Verkehrsinfrastrukturen 25

3.1.10 Neue Gefahren und Herausforderungen für die Stabilität des Gesundheitssystems in Österreich durch neu oder vermehrt auftretende Infektionskrankheiten und allergieauslösende Neobiota (z.B. vektorenübertragene Krankheiten, Zoonosen,…) 27

3.1.11 Surveillance und Gewährleistung von Trinkwasser-Sicherheit und Wasser-Qualität 28

3.1.12 Evidenzbasierte Governance-Plattform zur Entscheidungsfindung im Krisenmanagement 29
3.1.13 Hitze und Unwetter als Risiko: Resilienz und Krisenfestigkeit des Gesundheitswesens sicherstellen 31
3.1.14 Disaster Nursing - Sicherstellung von Pflege in Krisensituationen 32
3.1.15 Schutz kritischer Infrastruktur im Bereich AMR und Sicherstellung einer antimikrobiellen Therapie 34
3.1.16 Innovatives Datenmanagement zur Bedarfs- und Distributionsplanung kritischer Medizintechnikprodukte in Krisensituationen 35
3.1.17 Austausch interoperabler Daten im Bereich Krisen- und Katastrophenmanagement 36
3.1.18 Entscheidungsunterstützung für Einsatzkräfte 38
3.1.19 Klimaresilienz von grundwasserbasierten Wasserversorgungsanlagen in Österreich 40
3.1.20 Schutz kritischer Infrastruktur allgemein 41
3.2 KIRAS. Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für F&E-Dienstleistungen 42
3.2.1 Verschwörungsnarrative und ihre „Attraktivität“ für die Generation 45+ 42
3.2.2 Akzeptanz von intelligenten Überwachungs- und Identifikationssystemen im öffentlichen Raum 43
3.2.3 Entwicklung von Maßnahmen zur Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (RKE-Richtlinie 2022) 44
3.2.4 Risikopotenzial und Kontextfaktoren von jugendlicher Delinquenz und Viktimisierung in Bezug auf familienbasierte Formen von Kriminalität mit spezieller Berücksichtigung von Tendenzen soziökonomischer Marginalisierung in Migrationspopulationen 45
3.2.5 Stärkung der Rechtssicherheit durch Vereinheitlichung der Anforderungen an die interprofessionelle Zusammenarbeit zwischen der Polizei und Dolmetscherinnen und Dolmetschern in der Kommunikationsüberwachung 46
3.2.6 ABC-UAV-Freisetzung 48
3.2.7 C-UAS Demonstrator 49
3.2.8 Hochwasser- und Energieversorgungssicherheit an größeren Flüssen mit intensiver Wasserkraftnutzung im Spannungsfeld nutzungsbeeinflusster Sohlveränderungen und deren Auswirkung auf die Wassersversorgungs-sicherheit unter Berücksichtigung von Einflüssen des Klimawandels 50
3.2.9 Effiziente Frühwarn- und Alarmsysteme bei Störfällen an Stauanlagen 51

3.2.10 Aufbau und Betrieb eines flächendeckenden Prognose- und Detektions- und Alarmierungssystems in ständiger Bereitschaft für Waldbrände in Österreich (BML) 52
3.2.11 Organisierte Kriminalität als Herausforderung für den Strafvollzug 53
3.2.12 Fremdenrecht und Strafrecht – Schnittpunkte und wechselseitige Abhängigkeiten 54
3.2.13 Haftgestaltung für Frauen und Jugendliche durch sicherheitsarchitektonische Elemente 55
3.2.14 Konzeptuelle Weiterentwicklung des Konzepts der wirtschaftlichen Landesverteidigung in einem europäischen Kontext 56
3.2.15 Erhebung des Versorgungsbedarfes von Blaulicht- und anderen krisenrelevanten Organisationen 58
3.2.16 Föderierter Datenraum für GSVP-Missionen 59
3.2.17 Rechtlicher Anpassungsbedarf sowie gesamtgesellschaftliche Aspekte im Zuge der Notfallplanung zur besseren Nachverfolgbarkeit von Ausbrüchen lebensmittelbedingter sowie sonstiger übertragbarer Infektionskrankheiten durch Rückgriff auf Nutzer:innen-Daten im Anlassfall (wie z.B. Kundenkarten, Bewegungsdaten etc.) 60
3.2.18 Klimaschutz als zentrale Basis für die umfassende Sicherung der Infrastruktur im Gesundheitssektor und der Gesundheitsversorgung 61
3.2.19 Psychosoziale Resilienz der Beschäftigten in kritischen Infrastrukturen 62
3.2.20 Early Warning Tool zur Bewertung internationaler Versorgungsunterbrechungen der österreichischen Agrargüter- und Lebensmittelproduktion 65
3.2.21 Wissensmanagementsysteme zur effizienten Entwicklung von Strategien im Sicherheitsbereich 66
3.2.22 Explorationsstudie zu einem kompakten und einfach einsetzbarem Spürroboter für Einsatzkräfte 66
3.2.23 Chancen und Möglichkeiten für den Aufbau einer „Community of Users“ für die zivile Sicherheitsforschung in Österreich 68
3.2.24 Informelle Hilfe in Krisenzeiten 69
3.2.25 Geistige Landesverteidigung – Vorwissen und Interessen von Schülerinnen und Schülern der Sekundarstufen I und II an sicherheitspolitischen Fragestellungen 70
3.2.26 Krisen- und Katastrophenforschung – Aktuelle Entwicklungen sowie Aus-, Fort- und Weiterbildung in Österreich 72
3.2.27 Implementierung eines automatischen Detektierungs- und Warnsystems zum Sedimentmanagement von Schlüsselbauwerken der alpinen Schutzinfrastruktur 73
3.2.28 Schutz kritischer Infrastruktur allgemein 74

3.3 K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für kooperative F&E-Projekte 75
3.3.1 Die zukünftige Entwicklung kryptographischer Verfahren 75
3.3.2 Förderung des Wissensaustauschs in Strafverfolgungsbehörden durch NLP- und LLM-basierte Chatbots 76
3.3.3 Mobile digitale Aufnahme von Schuhspuren 77
3.3.4 Entwicklung einer KI-unterstützten Werkspurensuche 78
3.3.5 Virtual- / Mixed Reality Tool für die Bewertung von Umweltkatastrophen, zugehörige Maßnahmenplanung sowie die Post-Disaster Schadenserhebung 79
3.3.6 Prozessierungsframework für Lidar und bildgebende multimodale Sensordaten 80
3.3.7 Entwicklung eines Kryptosystems, welches mit österreichischem Wissen entwickelt und zukünftig im österreichischen Wirtschaftssystem produziert wird. Im Bereich der Cyber-Sicherheit ist die Verschlüsselung der Garant zur Gewährleistung des Schutzziels Vertraulichkeit 81
3.3.8 Die effiziente Behandlung digitaler Beweismitteln 82
3.3.9 Prison Intelligence als Mittel zur Erhöhung der dynamischen Sicherheit in Justizanstalten 85
3.3.10 Sichere technologieunterstützte (Re-)Integration 86
3.3.11 Mixed Reality-unterstütztes Training für die Vorbereitung auf Einsätze in Krisensituationen 88
3.3.12 Effizientere und zielgerichtetere Kontrollen im Internet für einen verbesserten Verbraucher:innenschutz entlang der Lebensmittelkette – Forschung im Bereich Mystery Shopping und Web-Crawler-Entwicklung für Zwecke der Betrugsprävention und Marktüberwachung 89
3.3.13 Sichere Sekundärnutzung von Gesundheitsdaten für resiliente Gesundheitssysteme 91
3.3.14 Cybersicherheit für Fahrzeuge 92
3.3.15 Bekämpfung von Desinformation durch die Analyse und Detektion von Fake-News-Netzwerken 93
3.3.16 Cybersicherheit allgemein 94
3.4 K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für F&E-Dienstleistungen 95
3.4.1 Definition von Anforderungen für QKD-Lösungen für das Zentrale Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau 95
3.4.2 Fachkräftebedarf im Bereich der Cybersicherheit 96
3.4.3 Steigerung der Cybersicherheit und Resilienz landwirtschaftlicher Prozesse und Systeme zur Gewährleistung der Versorgungssicherheit Österreichs 97
3.4.4 Entwicklung eines OpenSource-Frameworks (EUPL lizenziert) zu Murensimulationen mit Schwerpunkt auf österreichische Verhältnisse 98

3.4.5 Data Science und KI für Trendanalysen von Mediendaten in seltenen Sprachen 99
3.4.6 Cybersecurity-Literacy – Wissensvermittlung in der oberen Sekundarstufe in Österreich 100
3.4.7 Instrumente zur Bewertung der rechtlichen, technischen und ethischen Einsatzmöglichkeiten von KI-gestützten Technologien in eJustice Anwendungen 101
3.4.8 Cybersicherheit allgemein 103
3.5 KIRAS/K-PASS F&E-Dienstleistung Innovation AKUT 103

4 INSTRUMENTE UND ANFORDERUNGEN 105
4.1 Kooperatives F&E-Projekt 105
4.1.1 Konsortien 105
4.1.2 Forschungskategorien 106
4.2 F&E-Dienstleistung 106
4.2.1 Allgemein 106
4.2.2 Bietergemeinschaften 107
4.2.3 Auflagen und Bedingungen durch Jury 107
4.2.4 Weitere Anforderungen und Vorgaben zur Einreichung von F&E-Dienstleistungen 108

5 AUSSCHREIBUNGSDOKUMENTE 109

6 FÖRDERUNGS-/FINANZIERUNGSENTSCHEIDUNG UND RECHTSGRUNDLAGEN 111

7 WEITERE INFORMATIONEN 111
7.1 Hinweise zum Kostenplan 111
7.2 Service FFG Projektdatenbank 112
7.3 Open Access Publikationen 112
7.4 Umgang mit Projektdaten – Datenmanagementplan 113
7.5 Weitere Förderungsmöglichkeiten der FFG 113

8 ANHANG: CHECKLISTE FÜR DIE ANTRAGSEINREICHUNG ... 114

TABELLENVERZEICHNIS

Tabelle 1: Instrumente und Ausschreibungsschwerpunkte 9
Tabelle 2: Beratungsmöglichkeiten.....10
Tabelle 3: Ausschreibungsdokumente 110
Tabelle 4: Formalprüfungscheckliste 114

1 DAS WICHTIGSTE IN KÜRZE

Im Rahmen von **KIRAS/K-PASS** stehen für die kommende Ausschreibung 13,8 Millionen EUR zur Verfügung.

Einreichung:

Projektanträge sind bei der Österreichischen Forschungsförderungsgesellschaft (FFG) bis spätestens 01.03.2024, für die KMU-Initiative Innovation AKUT- bis 31.01.2024, einzubringen. Eventuelle weitere Termine für Innovation AKUT werden noch bekanntgegeben. Die Einreichung ist ausschließlich via eCall möglich und hat vollständig und rechtzeitig bis zum Ende der Einreichfrist zu erfolgen. Eine spätere Einreichung (nach 12:00 Uhr des genannten Tages) wird nicht mehr angenommen und führt automatisch zum Ausschluss aus dem Auswahlverfahren.

Tabelle 1: Instrumente und Ausschreibungsschwerpunkte

Förderungs-/ Finanzierungsinstrument	Kooperatives F&E Projekt	F&E-Dienstleistung	F&E- Dienstleistung KMU-Initiative Innovation AKUT
Kurzbeschreibung	Kooperatives F&E Projekt Industrielle Forschung (IF) oder Experimentelle Entwicklung (EE)	Erfüllung eines vorgegebenen Ausschreibungs-inhaltes	Innovatives Projekt mit KMU-Beteiligung, TRL 6-8
Schutz kritischer Infrastruktur (KIRAS)	Ja Siehe Kapitel 3.1	Ja Siehe Kapitel 3.2	Ja Siehe Kapitel 3.5
Cybersicherheit (K-PASS)	Ja Siehe Kapitel 3.3	Ja Siehe Kapitel 3.4	Ja Siehe Kapitel 3.5
Beantragte Förderung in €	min. 100.000 bis max. 2 Mio. €	keine Vorgabe	max. 100.000 € inkl. ev. UST
Finanzierungsquote	nicht anwendbar	100%	100%
Förderungsquote	max. 85%	nicht anwendbar	nicht anwendbar
Laufzeit in Monaten	max. 24 (und 12 Monate max. kostenneutrale Fristerstreckung)	max. 24 (und 12 Monate max. kostenneutrale Fristerstreckung)	max. 12 Monate (und ggf. kostenneutrale Fristerstreckung in Ausnahmefällen)
Kooperationserfordernis	ja	nein	ja
Sprache	Deutsch	Deutsch	Deutsch
Einreichfrist	01.03.2024	01.03.2024	31.01.2024
Zum Einreichportal	eCall		

Tabelle 2: Beratungsmöglichkeiten

Name	Kontaktdaten	Beratung zum Thema
Christian Brüggemann, MLS	Tel.: +43577555071 E-Mail: christian.brueggemann@ffg.at	Allgemeine Einreichberatung
Jozef Janco, MSc.	Tel.: +43577555073 E-Mail: jozef.janco@ffg.at	Allgemeine Einreichberatung
Dr. Polina Wilhelm	Tel.: +43577555072 E-Mail: polina.wilhelm@ffg.at	Allgemeine Einreichberatung
Mag. Gabriela Baluszynska	Tel.: +43577556092 E-Mail: gabriela.baluszynska@ffg.at	Kostenfragen
Mag. Martin Hudecek	Tel.: +43577556091 E-Mail: martin.hudecek@ffg.at	Kostenfragen

Inhaltliche Beratungsgespräche allgemeiner Natur können auf Wunsch eines potenziellen Antragstellers bis 16.02.2024 geführt werden. Terminvereinbarungen sind bis spätestens 02.02.2024 in schriftlicher Form an Herrn Christian Brüggemann (christian.brueggemann@ffg.at) zu stellen.

Formal- und Vertragsfragen sind ausschließlich schriftlich per E-Mail an Herrn Christian Brüggemann (christian.brueggemann@ffg.at) bis 02.02.2024 zu stellen.

Weiterführende Informationen:

- www.ffg.at/kiras
- www.kiras.at
- www.ffg.at/k-pass
- www.ffg.at/sicherheitsforschung
- www.ffg.at/kiras-k-pass-innovation-akut

Information zur Einstufung in die Forschungskategorie:
Im Rahmen der Antragstellung wird das Vorhaben in die Forschungskategorie Industrielle Forschung oder Experimentelle Entwicklung eingestuft. Die Einstufung wird im Rahmen der Begutachtung geprüft und kann gegebenenfalls vom Bewertungsgremium geändert werden.
Beachten Sie im Rahmen der Antragstellung die näheren Erläuterungen zu den Forschungskategorien „Industrielle Forschung“ und „Experimentelle Entwicklung“, sowie die ergänzenden Angaben zu den TRLs (Technology Readiness Levels) im Anhang des Leitfadens für Kooperative F&E-Projekte (v4.3).

Bitte beachten Sie:
Sind die Formalvoraussetzungen für eine Projekteinreichung entsprechend den Konditionen und Kriterien des jeweiligen Förderungsinstruments nicht erfüllt und handelt es sich um nicht-behebbare Mängel, wird das Förderungsansuchen bei der Formalprüfung aufgrund der erforderlichen Gleichbehandlung aller Förderungsansuchen ausnahmslos aus dem weiteren Verfahren ausgeschieden und formal abgelehnt.

2 MOTIVATION

2.1 Hintergrund KIRAS

Das nunmehr unter der Programmverantwortung des Bundesministeriums für Finanzen (BMF) stehende österreichische Sicherheitsforschungsförderprogramm „KIRAS“ (KIRAS leitet sich aus dem Griechischen ab und setzt sich zusammen aus den Worten kirkos (Kreis) und asphaleia (Sicherheit)). „Kreis“ ist in diesem Fall als integrativ zu verstehen, da im Rahmen des KIRAS- Programms alle Disziplinen und Dimensionen miteingeschlossen werden) unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der Sicherheit Österreichs und seiner Bevölkerung. Das BMF hat die Österreichische Forschungsförderungsgesellschaft (FFG) mit dem Programm- und Schirmmanagement für das KIRAS- Programm beauftragt.

Die Gewährleistung von „Sicherheit“ ist eine staatliche und daher ressortübergreifende Kernaufgabe. Vor dem Hintergrund vielfältiger, sich in stetem Wandel befindlicher Bedrohungslagen für unsere Gesellschaft gilt es, innovative Ansätze für die Begegnung dieser Bedrohungen zu entwickeln. Darin manifestiert sich die unbedingte Notwendigkeit eines Beitrages von Forschung und Innovation bei der Begegnung der Herausforderung „Gewährleistung von Sicherheit“.

In KIRAS erfolgt die thematische Konzentration auf F&E-Projekte der Sicherheitsforschung, die den Schutz von kritischen Infrastrukturen behandeln.

Zusätzlich werden innerhalb dieses generellen Schwerpunkts für jede Ausschreibung spezifische Forschungsschwerpunkte durch die sicherheitspolitisch verantwortlichen Ressorts festgelegt. Diese Spezifizierung erlaubt es Einreichern, zielgerichtet den aktuellen Bedarf anzusprechen.

Die Sektoren, die als kritische Infrastrukturen gelten, sowie die strategischen Ziele sind in der KIRAS-Sonderrichtlinie beschrieben.

Im Thema Sicherheit (KIRAS) werden grundsätzlich solche sicherheitsforschungsrelevanten Vorhaben gefördert, die inhaltlich nicht effektiv durch andere bestehende Förderinitiativen abgedeckt werden können (z.B. in den Themenbereichen Energie, Mobilität und Verkehr, Informations- und Kommunikationstechnologien, Produktion und Raumfahrt). Im Sinne einer umfassenden Umsetzung des Themenmanagements erfolgt eine Abstimmung nicht nur mit Forschungsprogrammen innerhalb des BMF sondern mit allen im Lenkungsausschuss vertretenen Stakeholdern (Ministerien, Interessensvertretungen, RFTE, u.a.).

Die enge Verzahnung mit der Sicherheitspolitik (Schwerpunktsetzung, Auswahlverfahren, etc.), die in KIRAS wie in keiner anderen Förderinitiative gegeben ist, erlaubt in einem technologieoffenen Ansatz die ausschließliche Fokussierung auf sicherheitsrelevante Themen (i.S.v. „security“).

KIRAS weist folgende Alleinstellungsmerkmale auf:

- Definition von Sicherheit als nationale Sicherheit
- Beforschung sicherheitspolitisch relevanter Vorhaben im zivilen und dual-use-Bereich
- der integrative, umfassende Ansatz
- die Einbeziehung von Bedarfsträgern der Sicherheitspolitik
- ein klarer Österreichbezug
- die zwingende projektbezogene Integrierung von GSK- Aspekten
- die Möglichkeit der Klassifizierung von Projekten.

KIRAS wird keine Rüstungsforschung betreiben und sich klar von Rüstungsforschung abgrenzen. Das KIRAS-Programm hat einen eindeutigen und klaren zivilen Programmfokus, da Sicherheitsforschung hinsichtlich seiner verteidigungspolitischen Anforderungen keine wehrtechnisch orientierte Materie ist. Die Abgrenzung zwischen Rüstungs- und Verteidigungsforschung einerseits und Sicherheitsforschung andererseits erfolgt im Rahmen des Nationalen Sicherheitsforschungsprogramms in Übereinstimmung mit der diesbezüglichen Abgrenzung der EU im Rahmen des Europäischen Sicherheitsforschungsprogramms.

Das Verteidigungsforschungsprogramm FORTE ist ausschließlich auf den militärischen Kernbereich ausgerichtet und deckt all jene sicherheitspolitisch relevanten Forschungsthemen ab, die beim nationalen Sicherheitsforschungsprogramm KIRAS keine Berücksichtigung finden können. FORTE ist somit komplementär zu KIRAS zu sehen und umzusetzen, da:

- diese Themenmaterie gem. KIRAS-Sonderrichtlinie entweder dezidiert ausgeschlossen ist (KIRAS hat einen zivilen Programmfokus mit klarer Abgrenzung zur Rüstungs- und Verteidigungsforschung - d.h. keine Rüstungsforschung) oder
- das ÖBH, als Bedarfsträger, ein thematisches Alleinstellungsmerkmal hat, welches nicht im prioritären Interesse anderer sicherheitsrelevanter Bedarfsträger liegt, vom ÖBH aber dennoch zur Erfüllung ihrer Aufgaben unbedingt benötigt wird.

2.2 Hintergrund K-PASS

Im Rahmen der „Österreichischen Sicherheitsklammer“ bietet das Programm KIRAS/ „Kybernet-Pass“ (im folgenden K-PASS), unter der Programmverantwortung des Bundesministeriums für Finanzen (BMF), eine Unterstützung für nationale Forschungsvorhaben mit dem Ziel der Erhöhung der digitalen Sicherheit Österreichs und seiner Bevölkerung.

K-PASS unterstützt österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien und der Gewinnung des erforderlichen Wissens, um die digitale Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren. Ziel ist die Schaffung marktnaher Forschungsergebnisse zu digitaler Sicherheit für Sicherheitsanwender.

K-PASS ist Teil der „Österreichischen Sicherheitsklammer“ des BMF und stellt gemeinsam mit KIRAS und FORTE die koordinierte Umsetzung eines österreichischen Sicherheits- und Verteidigungsforschungs-Programmrahmens sicher.

Der Schwerpunkt der Förderaktivitäten in K-PASS wird in der ersten Phase (2023-2027, in Anlehnung an das Europäische Forschungsrahmenprogramm Horizont Europa) in den folgenden Bereichen liegen:

- Sicherheit von „security“-relevanter Software
- Sicherheit von „security“-relevanter Hardware
- Schutz für IoT-Anwendungen und Netze
- Cyber Crime und Digitale Forensik
- E-Government-Schutz (inkl. Aufrechterhaltung des Vertrauens in der Bevölkerung)
- Steganografie und digitale Datenanalyse (z.B. Post-Quantenverschlüsselung)
- Der User als Teil der digitalen Dimension (inkl. Datensicherheit, Cyber-Stalking, Cyber-Mobbing)
- Sicherheit und Künstliche Intelligenz
- Hybride Bedrohungen
- Schutz für IKT-Systeme als „smarte“ kritische Infrastruktursysteme (z.B. autonome Mobilität, smarte Strom- und sonstige Versorgungsnetze) inkl. Resilienz, Versorgungssicherheit und Vertrauensüberprüfung (vor allem Themen für Breitbandausbau und 5G/6G-Netze).

Zusätzlich werden innerhalb dieses generellen Schwerpunkts für jede Ausschreibung spezifische Forschungsschwerpunkte durch die sicherheitspolitisch verantwortlichen Ressorts festgelegt.

Detaillierte Information finden Sie in der K-PASS Sonderrichtlinie.

2.3 Zielgruppen und Förderwerber

KIRAS/K-PASS richtet sich an folgende Zielgruppen:

- Industrie- und Dienstleistungsunternehmen mit Unternehmensstandort oder Forschungsstätte in Österreich, sowie
- Forschungseinrichtungen, Forschende aus dem universitären und außeruniversitären Bereich, Fachhochschulen
- Österreichische öffentliche und private Bedarfsträger: Bedarfsträger sind öffentliche oder private Institutionen, die (Mit-)Verantwortung für die Gewährleistung von Sicherheit (im Sinne von „security“) als öffentliches Gut tragen und Bedarf an Ergebnissen der Sicherheitsforschung (Technologien, Studien, etc.) haben bzw. diese anwenden. Dazu zählen insbesondere:

- Sicherheitspolitisch verantwortliche Bundesministerien („Bedarfsträger der Sicherheitspolitik“)
- weitere Bundesministerien
- Bundesagenturen
- Bundes- und Landesbehörden
- Städte und Gemeinden
- Infrastrukturbetreiber
- Blaulichtorganisationen
- Vereine und Nicht-Regierungsorganisationen.

KIRAS/K-PASS wendet sich inhaltlich auch an Einrichtungen der österreichischen Bundesverwaltung. Diese Einrichtungen können zwar nicht als Förderungswerber auftreten, sind jedoch ermutigt, sich im Rahmen von Konsortialbildungen an Vorhaben im Rahmen von KIRAS/K-PASS zu beteiligen.

Förderwerber:

- Förderbar sind außerhalb der Bundesverwaltung stehende juristische Personen, Personengesellschaften oder Einzelunternehmen
- Natürliche Personen sind als Einreicher nur für das Instrument „F&E-Dienstleistungen“ zulässig.

2.4 Die Möglichkeit der Klassifizierung

Es besteht die Möglichkeit, einen Antrag auf Klassifizierung des Projektes zu stellen, wenn abzusehen ist, dass im Projekt mit klassifizierten Informationen gearbeitet werden soll. Klassifizierte Informationen sind Informationen, Tatsachen, Gegenstände und Nachrichten, die unabhängig von Darstellungsform und Datenträger eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen (siehe Informationssicherheitsgesetz und –Verordnung).

Für den Fall, dass der Antragsteller einen Antrag auf Klassifizierung stellt, wird dieser Antrag nach positiv bestandener Formalprüfung durch die FFG von der FFG über das BMF an die Verbindungspersonen zum Nationalen Sicherheitsrat (NSR) weitergeleitet, welche ihrerseits prüfen, ob das Projekt mit bestehenden oder geplanten Systemen kompatibel ist und ob es wirklich als ein klassifiziertes Projekt durchgeführt werden muss. Wenn die Verbindungspersonen zum NSR feststellen, dass der Klassifizierungsantrag zu Recht gestellt wurde, erfolgt eine Prüfung durch den Kontrollbeauftragten, ob der Antragsteller die Schutzmaßnahmen laut Informationssicherheitsverordnung (bauliche und personelle Maßnahmen) ergriffen hat. Ist dies nicht der Fall, muss der (Projekt-)Antrag abgelehnt werden.

Wird der Antrag auf Klassifizierung von den Verbindungspersonen zum Nationalen Sicherheitsrat (NSR) negativ beschieden, wird das Projekt wieder der FFG zugeleitet und kann nach Rücksprache mit dem Antragsteller dem weiteren (normalen) Begutachtungsverfahren unterworfen werden.

Der Projektantrag darf keinesfalls klassifizierte Informationen enthalten.

Bitte lesen Sie die Rechtsgrundlagen, insbesondere die Anforderungen an Personal und bauliche Maßnahmen, wie sie in der Informationssicherheitsverordnung dargelegt sind, eingehend. Sollte der Antrag als „klassifiziert“ eingestuft werden, die baulichen und personellen Anforderungen aber nicht vorhanden sein, muss das Projekt abgelehnt werden. Die Informationssicherheitsverordnung kann von der KIRAS-Homepage heruntergeladen werden.

3 AUSSCHREIBUNGSSCHWERPUNKTE

Das Vorhaben muss sich prioritär auf einen der in Folge beschriebenen Ausschreibungsschwerpunkte beziehen, kann aber auch mehrere dieser Schwerpunkte ansprechen. Die folgenden Ausschreibungsschwerpunkte sind allerdings nicht ausschließlich zu begreifen. Es können auch weiterhin alle kooperativen Projekte, beziehungsweise F&E-Dienstleistungen eingereicht werden, welche dem Schutz kritischer Infrastruktur/Cybersicherheit gelten.

Um die zukünftige Einsatzfähigkeit von angewandten Forschungsideen zu erhöhen, wird den Antragstellern empfohlen, in den Projektanträgen zu beschreiben, wie die geltenden rechtlichen Rahmenbedingungen im beforschten Themengebiet aussehen. Weiters sollte dargelegt werden, ob und welche Rechtsvorschriften einer praktischen Umsetzung der Forschungsergebnisse entgegenstehen könnten bzw. welche Anpassungen in den Rechtsgrundlagen dies ermöglichen / vereinfachen würden. Die dazu erforderliche rechtliche Expertise kann sowohl von den Konsortialmitgliedern direkt als auch im Subauftrag in die Forschungsprojekte eingebracht werden.

Folgend sind die Ausschreibungsschwerpunkte aus sicherheitspolitischer Sicht beschrieben.

3.1 KIRAS. Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für kooperative F&E-Projekte

3.1.1 Innovative multimodale und multisensorale Monitoringlösungen durch UAVs mit alternativen Antriebssystemen

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Die Überwachung sicherheitsrelevanter Gebiete und Infrastrukturen gewinnt vor dem Hintergrund von sich sehr dynamisch veränderten Bedrohungssituationen stark an Bedeutung. Gefahrenlagen sind dabei nicht unbedingt lokal beschränkt, sondern können mehrere Objekte bzw. ganze Regionen betreffen. Innovative technische Assistenzsysteme müssen daher eine rasche/flexible Einsetzbarkeit und teil-/autonome Unterstützung gewährleisten und es somit ermöglichen gezielt kritische Infrastrukturobjekte als auch größere Gebiete mit geringem Personaleinsatz effektiv überwachen zu können.

Innovative UAV-Lösungen mit alternativen Antriebssystemen bieten die Möglichkeit einer deutlichen Leistungssteigerung (Einsatzdauer, Traglast) und ermöglichen damit auch völlig neue Einsatzstrategien für Monitoringaufgaben. Um ein gezieltes, permanentes und flexibles Monitoring von kritischen Infrastrukturen und sicherheitsrelevanten Gebieten zu ermöglichen, ist der Einsatz unterschiedlicher Sensorik erforderlich. Optische, thermale, Radar und hyperspektrale Sensorlösungen bieten in Kombination mit präzisen GNSS-Lösungen eine optimale Datengrundlage für KI-basierte Analyseansätze und die echtzeitnahe Ableitung von umfassender Lageinformation für unterschiedliche Aufgaben und Einsatzszenarien. Kooperative Lösungsansätze unter Einbindung von heterogenen (teil-)autonomen UAVs ermöglichen auf Basis sich ergänzender Systemeigenschaften eine zielgerichtete Unterstützungsleistung der Einsatzkräfte.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Innovative Entwicklungen und Adaptionen für alternative UAV-Antriebssysteme zur Erhöhung der Einsatzdauer und Traglast
- Innovative, modulare Integrationsmöglichkeiten („hook-up“ Konzept) von leistungsfähiger und präziser Sensorik (optisch, thermal, Radar, Hyperspektral, GNSS) in eine UAV-Sensorplattform und gezielten Plattformansteuerung für Nadir- und Oblique-Aufnahmeszenarien
- Entwicklung eines kooperativen und kollaborativen Managementansatzes für den optimierten Einsatz von mehreren UAVs mit unterschiedlichen Fähigkeiten (Sensorik, Einsatzdauer, etc.) für eine effiziente, teilautonome Bearbeitung von Monitoringaufgaben
- Einsatz von robusten und innovativen Kommunikationslösungen auf Basis von 5G-Technologien für innovative Kooperationsansätze zwischen den einzelnen Modulen und einer Einsatzzentrale

- Entwicklung von semantischen echtzeitfähigen Algorithmen und Methoden für die Detektion sowie automatisierte, KI-basierte Datenanalyse sowie „Change-Detection“-Ansätzen
- Georeferenzierung der multisensoralen Daten mit unterschiedlichen Aufnahmewinkel und Zusammenführung der zeit- und geo-orientierten Informationen zu einem Lagebild
- Generierung eines Moduls zur simulationsunterstützten Vor-Ort-Systeminstallation und -kalibrierung (Sichtbarkeitsanalysen, Licht-/Wettersituation, modulbezogene Aufgabenverteilung, etc.)
- Möglichkeiten zur Einbindung der Daten und Analyseergebnisse in andere Systeme auf Basis von Standardschnittstellen
- Sozialwissenschaftliche Analyse zur Akzeptanz (teil-)autonomer technologischer Lösungen seitens der Einsatzkräfte und der Bevölkerung.

Eine Berücksichtigung und Verwertung von Teil-/Ergebnissen aus Forschungsaktivitäten ist für ein Projektvorhaben, das zum gegenständlichen Ausschreibungsschwerpunkt eingereicht werden soll, besonders wichtig. Von besonderer Relevanz sind dabei die kooperativen KIRAS F&E-Projekte WatchDog, UASwarm, KI-Secure, NRT-COP.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.2 Kontaminationsmonitor - Feststellung von Kontaminationsrückständen mit optischen Detektionsmethoden

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsfoschung@bmlv.gv.at

Nach einer Freisetzung von ABC-Gefahrstoffen ist davon auszugehen, dass Personen und Ausrüstung potentiell kontaminiert sind und dementsprechend dekontaminiert werden müssen.

Besonders bei Zivilpersonen, die überraschend und unvorbereitet betroffen sind, wird eine schnelle Feststellung benötigt. Bei Massenanlassfällen könnte mit einer solchen Detektionsmethode die Triage, wer Dekontamination benötigt und wer nicht, maßgeblich unterstützt werden. Damit würde die meistens limitierten Dekontaminationskapazitäten entlastet und zielgerichtete Hilfe erfolgen. Gleichzeitig würde ein solches Verfahren ermöglichen, die Effektivität der Dekontamination nachweisen zu können.

Bei Ausrüstungsgegenständen ist die Feststellung von Oberflächenkontamination sinnvoll, um diese im positiven Fall (nicht kontaminiert) direkt wieder zum Einsatz bringen zu können oder nur die betroffenen Stellen dekontaminieren zu müssen.

Im radiologischen Bereich kann man Personen bzw. Gegenstände mit entsprechenden Geräten „freimessen“ und dann können diese ohne Dekontamination passieren bzw. wiederverwendet werden.

Im biologischen/chemischen Bereich könnte so ein „Freimessen“ über optische Methoden und Algorithmus-unterstützte Auswertung im multispektralen Bereich erfolgen. Bei Tatorten werden beispielsweise verschiedene Lichtwellenlängen und verschiedene additive Substanzen benutzt, um optisch Spuren wie Blut, Fingerabdrücke, Schmauch, Körperflüssigkeiten oder Treibstoff zu detektieren.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Können biologische und/oder chemische Gefahrstoffe optisch/spektral detektiert werden?
- Sind diese Methoden empfindlich genug, um eine Oberfläche als nicht kontaminiert einzustufen und wie kann die Empfindlichkeit der Methoden gesteigert werden?
- Können diese Methoden unter Einsatzbedingungen bei Personen angewendet werden (in Echtzeit, hochmobil, hautverträglich, unter Reduktion/Ausschluss störender Effekte wie Streulicht etc.)?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.3 Technische Möglichkeiten zur Personalreduktion beim Schutz kritischer Infrastruktur

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Ein wesentlicher Teil der Schutzoperation ist der Schutz "Kritischer Infrastruktur". Es gibt je nach Bundesland mehrere definierte nationale und regionale Schutzobjekte, welche vor allem für die Informationsweitergabe und Versorgungssicherheit von Bedeutung sind. Ein Ausfall dieser Infrastruktur kann massive Nachteile für die Stabilität der Region mit sich bringen.

Der entsprechende Schutz, vor allem die Bewachung und Verteidigung, ist jedoch personalintensiv. Die Herausforderung lautet daher: möglichst hoher Schutz der "Kritischen Infrastruktur" bei möglichst wenig Personal.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie kann man mit technischen (z. B. Überwachungssysteme, Sensoren, …) und sonstigen Mitteln (z. B. Pionier- bzw. Bautechnischer Art) den Schutz „Kritischer Infrastruktur“ möglichst optimieren, um einerseits einen hohen Schutz zu erzielen und andererseits möglichst viel Personal vor Ort einzusparen (Ökonomie der Kräfte). Dies unter den Gesichtspunkten Sparsamkeit, Einfachheit und relativ rasche Errichtung (Machbarkeit).
- Wie kann man die Auswirkungen der „neuen“ Bedrohungen, Möglichkeiten und Chancen der technologisch naturwissenschaftlichen Entwicklungen (z.B. Kampf um und mit Information, Drohnen, Robotik, künstliche Intelligenz) berücksichtigen

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.4 Erhebung und Berechnung von geologischen sowie geographischen Daten mittels der Kombination von Feldmethoden und der Geoanalyse von Satellitenbildern

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsfoschung@bmlv.gv.at

Die Geländebeurteilung ist zentraler Bestandteil des Führungsprozesses auf militärischen und zivilen Entscheidungsebenen. Um eine rasche Verfügbarkeit von präzisen Geländedaten sicherzustellen, fungiert u.a. das Militärische Geowesen als integraler Bereitsteller von Geodaten und Expertise im geowissenschaftlichen Bereich. Erhöhte einsatzspezifische Anforderungen an eine "klassische Geländeanalyse" durch komplexe Szenarien oder sich rasch verändernde Umweltbedingungen (z.B. durch den Klimawandel) bedeuten daher eine Notwendigkeit für ständige Weiterentwicklung der Methoden u.a. im Militärischen Geowesen.

Bisher wurden Geländeanalysen überwiegend auf der Basis von Geländehöhenmodellen und, soweit vorhanden, geologischer und bodenkundlicher Daten berechnet, obwohl viele andere Geländefaktoren ebenfalls wesentlich sind. Problematisch ist in diesem Zusammenhang vor allem die Verfügbarkeit von digitalen aber auch analogen Geodaten. Während im Inland auf Dienste wie die Geologische Bundesanstalt oder die Zentralanstalt für Meteorologie und Geodynamik zurückgegriffen werden kann, ist die Datenlage im Einsatzgebiet außerhalb Österreichs unbefriedigend.

Um bestehende Dienstleistungen und Produkte u.a. des Militärischen Geowesens im Sinne der Bedarfsträgerorientierung zu verbessern, müssen neue Methoden der Geodatenbeschaffung und -analyse entwickelt, sowie bestehende Methoden optimiert werden.

Hier bieten sich vor allem geowissenschaftliche Feldmethoden an, mit denen die Daten für ein besseres Verständnis der Geländeeigenschaften eines Einsatzraumes erhoben werden können. Besonders die Ableitung von Geodaten aus multispektralen Satellitenbildern bietet enormes Potential für einsatzspezifische Geoanalysen ohne Personaleinsatz vor Ort.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können geomorphologische Strukturen (als wichtiger Faktor nach Höhenmodell, Geologie und Bodenkunde) insbesondere in der Fernerkundung erhoben werden und welche Methoden eignen sich am besten für eine zeitnahe, akkurate und bedarfsträgerorientierte Analyse und Darstellung der Daten?
- Welche Bedeutung (taktisch, operativ, strategisch) haben in Geländeanalysen berechnete und dargestellte Strukturen?
- Welcher Zusammenhang besteht zwischen physischen und humangeographischen Geofaktoren?

Wichtig ist hierbei, bestehende Ergebnisse auslaufender oder bereits abgeschlossener KIRAS- Projekte zu berücksichtigen und vorhandene Synergien und Ergebnisse zu nutzen. Eine Zusammenarbeit mit den österreichischen Geodiensten ist für den Projekterfolg notwendig.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.5 Early Warning Tool für Lieferkettenunterbrechungen für Lebensmittel

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abteilung II/8 (BML)
E-Mail: abt-28@bml.gv.at

Voraussetzung für das Ergreifen von Lenkungsmaßnahmen, im Falle von Versorgungsunterbrechungen der Lebensmittelversorgung, ist die Erstellung eines möglichst umfassenden Lagebildes basierend auf – soweit möglich – Echtdaten aus dem Versorgungssystem. Je früher dabei Störungen erkannt werden können, desto besser und wirkungsvoller können allfällig zu ergreifende abfedernde und lenkende Maßnahmen sein.

Mit dem Projekt SYRI (Systemisches Risikomanagement und Resilienzplanung für die österreichische Lebensmittel-Versorgungssicherheit) wird eine Daten-, Server- und Datenbankinfrastruktur erstellt, die es erlaubt Warenfluss- und Bestandsdaten auf täglicher Basis von Unternehmen der Lebensmittellieferkette und Registerdaten zu integrieren. So werden große Teile des Österreichischen Lebensmittelliefernetzwerkes für fünf essentielle Produktgruppen erstellt und auf Basis dieser ein systemisches Risikomonitoring, das es erlaubt, alle Betriebsstätten nach ihrem Risiko, das sie für die Lebensmittelversorgung der österreichischen Bevölkerung auf regionaler Ebene darstellen, einzuteilen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erweiterung des systemischen Risikomonitorings nach der entwickelten Methode auf weitere essentielle Lebensmittelgruppen und wichtige Vorleistungen
- Bereitstellung von Informationen zu (drohenden) Lieferkettenunterbrechungen für teilnehmende Unternehmen und die mit Lenkungsaufgaben betrauten öffentlichen Stellen
- Entwicklung von Algorithmen zur Erstellung von zuverlässigen Prognosen über die Ausbreitung von Störungen im Lebensmittelliefernetzwerk und von Kommunikationsschnittstellen die die Störungsprognosen sicher an die betroffenen Unternehmen übermitteln können ohne sensitive Lieferketteninformationen preis zu geben
- Anwendung sowohl auf nationale, EU-weite und internationale Lieferkettenzusammenhänge/Handelsströme und Lieferkettennetzwerke (z.B. durch Web-Scraping einschlägiger Newsprovider).

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.6 Aufbau und Entwicklung einer innovativen Gebäudedatenbank zur Unterstützung der Analyse der physischen Verwundbarkeit von Gebäuden gegenüber Naturgefahren

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Sektion I – Wasserwirtschaft; Abteilung I/6 – Hochwasserrisikomanagement (BML)
E-Mail: martin.wenk@bml.gv.at

Obwohl Naturgefahrenprozesse bereits gut dokumentiert und in den Gefahrenkarten ausgewiesen sind, erfordern Risikoanalysen für das Siedlungsgebiet Daten zu exponierten Gebäuden (u.a. Anzahl, Bauweise, Bauperiode, Stockwerke, Hauptnutzungsart, Gebäudeöffnungen, Keller). Die physische Verwundbarkeit ist von den Gebäudeeigenschaften bestimmt und international gängige Modelle zur Abschätzung der Risiken erfordern sehr detaillierte lokale Gebäudedaten.

Das Gebäude- und Wohnungsregister (AGWR) der Statistik Austria verfolgt die Zielsetzung jedes Gebäude in Österreich zu erfassen. Unter dem Begriff „AGWR II“ ist die neu gestaltete Meldeschiene „Adress-GWR-Online" sowie das gemäß BGBl. I Nr. 125/2009 inhaltlich erweiterte Gebäude- und Wohnungsregister subsumiert. Hier werden, wenn vorhanden neben Adressdaten auch Daten über die Struktur von Gebäuden, Wohnungen und sonstigen Nutzungseinheiten geführt. Bei einigen für die Verwundbarkeit von Gebäuden interessanten Merkmalen wie der Bauweise ergibt sich, dass speziell bei älteren Gebäuden keine Daten im AGWR enthalten sind. Ziel ist die Erweiterung der Daten von Gebäuden (insb. hinsichtlich Bauweise, Bauperiode, Stockwerke, Hauptnutzungsart, Gebäudeöffnungen, Keller) sowie die Vertiefung des Wissens zu Unterschieden des Gebäudebestands auf lokaler und regionaler Ebene.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Methoden und Technologien zur Modularisierung von Informationen, sowie zur Integration externer und offener Informations- bzw. Wissensquellen
- Flexible und zuverlässige Extraktion von Gebäudeinformation aus strukturierten sowie unstrukturierten heterogenen Datenquellen
- Methoden und Technologien zur Schadensmodellierung und zum KI-gestütztem Ableiten von Schlussfolgerungen
- Entwicklung eines flexiblen und adaptiven Systems zur automatisierten Analyse und Klassifikation von unstrukturierten Daten aus unterschiedlichen Quellen unter Verwendung von Methoden der Künstlichen Intelligenz
- Verknüpfung und Visualisierung von Gebäudedaten für die Risikoanalyse insb. für Hochwasser, zur Verbesserung von Datenbeständen und Vergleichbarkeit im internationalen Kontext
- KI-gestützte Verbesserung der Ereignis- und Schadensdokumentationen, zur Vertiefung des Verständnisses von Schadensmustern auf lokaler Ebene (in Verbindung mit dem KIRAS Projekt CESARE)
- Bereitstellung eines Gebäudeinventars zur Bewertung von Risiken auf Gebäude-Ebene und Ableitung geeigneter Schadensfunktionen insbesondere in Hinblick auf unterschiedliche Gebäudekategorien und kritischer Infrastrukturen

- Anwendung einer monetären Schadensbewertung insb. für Hochwasser basierend auf dem abgeleiteten Gebäudebestand und Validierung der Ergebnisse.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.7 Netzwerkmodellierungen zur systemischen Risikobewertung der Lieferkettenabhängigkeiten kritischer Güter

Kontakt: Bundesministerium für Arbeit und Wirtschaft, Sektion VI – Nationale Marktstrategien, Referat VI/9a – Krisenmanagement, Ing. Mag. Michael Stern (BMAW)
E-Mail: michael.stern@bmaw.gv.at

Die Produktion eines großen Teils der kritischen Güter (Güter die wesentlich für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen sind) erfolgt mittlerweile in Abhängigkeit von einer Vielzahl von nationalen und internationalen Unternehmen, die in zunehmend komplexen Lieferbeziehungen miteinander verflochten sind. Unternehmen kennen jedoch häufig nur ihre direkten Zulieferer; bei den Partnerunternehmen der Zulieferer nimmt die Sichtbarkeit der Lieferketten typischerweise schnell ab. Daraus ergeben sich substantielle Abhängigkeiten, die erst dann bekannt werden, wenn es zu Störungen der Lieferketten kommt. Sollten solche Störungen kritische Zulieferer betreffen, also schwer ersetzbare Unternehmen von deren Produkten oder Dienstleistungen viele andere Unternehmen abhängen, besteht überdies ein systemisches Risiko, dass ursprünglich lokalisierte Störfälle zu Unterbrechungen bei mehreren kritischen Gütern führen können.

Das Ausmaß des Risikos durch solche Abhängigkeiten bei kritischen Gütern ist momentan nur unzureichend bekannt. Dadurch ist auch nur wenig bekannt, auf welche Länder sich diese Lieferkettenabhängigkeiten bei kritischen Gütern konzentrieren und welche geopolitischen Risiken damit einhergehen. Oftmals sind solche Informationen nur auf Basis von hochaggregierten Handels- oder Sektordaten verfügbar. Diese sind aber nicht hinreichend detailliert genug, um Aussagen über einzelne kritische Produkte bzw. die Unternehmen, die diese regional herstellen zu machen. Auch eine Klassifikation, welche Güter kritisch sind und welche nicht, lässt sich oft nicht eindeutig treffen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Güter sind für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen in Österreich am relevantesten (unter Berücksichtigung der Erkenntnisse von relevanten Vorprojekten wie z.B. KIRAS-Projekten ReaGtSion und e-Panini)? Und in welchen (österreichischen und internationalen) Regionen konzentrieren sich die Unternehmen, welche diese kritischen Güter herstellen?

- Mit welchen Datenquellen und Datenanalyseverfahren können die Netzwerke der Lieferkettenabhängigkeiten dieser Unternehmen in einem Detailgrad erfasst, rekonstruiert und modelliert werden, der über sektorale Klassifizierungen und aggregierte Produktkategorien aus Handelsdaten hinausgeht?
- Wie wahrscheinlich ist es, dass bestimmte lokalisierte Störungen sich auf diesen Netzwerken ausbreiten und zu einer nachhaltigen Reduktion der Verfügbarkeit einer oder mehrerer Kategorien von kritischen Gütern in Österreich führen?
- Wie können die Ergebnisse solcher Szenario- und Modellrechnungen in dynamische und interaktive Lagebilder (siehe z.B. KIRAS-Projekt DAGMAR) integriert werden, um den Entscheidungsträgern eine fortlaufend aktualisierte, umfassende und leicht verständliche Übersicht über Ausfallsrisiken unterschiedlicher Art zu bieten?
- Welche datenschutzrechtlichen Aspekte müssen bei dieser Art von Forschungsarbeit berücksichtigt werden, und wie kann die Einhaltung dieser Bestimmungen jederzeit sichergestellt und die Datensicherheit gewährleistet werden?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.8 Erstellung eines umfassenden Versorgungslagebilds im Sinne der Versorgungssicherungsgesetze durch einen abgestimmt kontrollierten Zugriff auf interne Unternehmensdaten im Krisenfall

Kontakt: Bundesministerium für Arbeit und Wirtschaft, Sektion VI – Nationale Marktstrategien, Referat VI/9a – Krisenmanagement, Ing. Mag. Michael Stern (BMAW)

E-Mail: michael.stern@bmaw.gv.at

Die Forschung geht davon aus, dass die Häufigkeit von Krisen, die etwa durch den Klimawandel, die wachsende Weltbevölkerung oder politische Ereignisse verursacht oder verstärkt werden, in Zukunft zunehmen wird. Zuletzt wurde durch die Covid-19-Pandemie wieder deutlich, dass Krisen, wenn sie eine bestimmte Größenordnung erreichen, massive volkswirtschaftliche Kosten verursachen und zu schweren gesellschaftlichen Verwerfungen führen können. Eine besondere Gefahr geht von Störungen bei der Bereitstellung von wichtigen Wirtschafts- und Bedarfsgütern aus. Mit dem Versorgungssicherheits- und dem Lebensmittelbewirtschaftungsgesetz wurden die rechtlichen Grundlagen geschaffen, damit die öffentliche Verwaltung im Krisenfall die Versorgung mit wichtigen Gütern sichergestellt werden kann. Um die richtigen Maßnahmen rasch ergreifen zu können, ist allerdings neben der Ermächtigung dazu auch ein klares Lagebild über die Versorgung unerlässlich, welches es erlaubt, vorhandene Datenbestände optimal einzusetzen und damit eine effiziente Lenkung zu ermöglichen. So soll im Krisenfall ein kontrollierter Zugriff auf Daten zum Bestand an wichtigen Gütern bei Handels- und Produktionsunternehmen gegeben sein. Im Nichtkrisenfall soll der Aufwand für Unternehmen minimal gehalten werden.

Der Zugriff und die Nutzung dieser Daten sind aus mehreren Gründen herausfordernd: zum einen ändern sich die Bestände laufend und daher kommen für Entscheidungen nur jene Daten in Frage, die auch den letztgültigen Stand widerspiegeln. Zum anderen liegen die Daten mitunter verteilt an unterschiedlichen Standorten und sind unterschiedlich strukturiert, wodurch die Integration dieser Daten komplex ist. Weiters sind sowohl die Speicherung als auch die Verarbeitung und die Übertragung kostenintensiv, weshalb eine anlasslose Verarbeitung oder Übertragung von Daten sowie die redundante Speicherung vermieden werden sollen. Schlussendlich sind die Daten aus Sicht der Unternehmen nur für den internen Gebrauch gedacht, da sie in falschen Händen zu Wettbewerbsnachteilen führen können.

In Anbetracht der genannten Herausforderungen und um die Verfügbarkeit eines Lagebilds auch in Extremsituationen gewährleisten zu können, wird ein Datenpool, also die Zusammenführung und zentrale Speicherung aller möglicherweise relevanten Daten, nicht als der effektivste und effizienteste Weg angesehen, um eine Basis für die datenbasierte Steuerung der Versorgung mit wichtigen Gütern zu schaffen. Es ist daher erforderlich, relevante Daten bei einem konkreten Anlassfall für Unternehmen transparent und nachvollziehbar abzufragen und effizient zur Ausgestaltung von Lenkungsmaßnahmen zu verarbeiten. So stellen etwa moderne, dezentrale Datenarchitekturen eine robuste und flexible Plattform dar und versprechen, die unternehmensübergreifende Nutzung von Daten zu ermöglichen, ohne dass für die Beteiligten große Aufwände entstehen oder ihre Datensouveränität unverhältnismäßig stark eingeschränkt wird.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Untersucht werden soll, welche Art von Datenarchitektur sich am besten eignet, um im Bedarfsfall optimal auf interne Unternehmensdaten zuzugreifen und diese zur Ausgestaltung von Lenkungsmaßnahmen nutzen zu können
- Neben den Anforderungen der öffentlichen Verwaltung sollen auch die Interessen der betroffenen Handels- und Produktionsunternehmen erhoben und unter der Maxime, dass Aufwand und Nutzen in einem vertretbaren Verhältnis stehen müssen, analysiert werden
- Aufwand und Nutzen sollen anhand von konkreten Anwendungsfällen bewertet und gegenübergestellt werden; betrachtet werden soll dabei, mit welchen Daten, unter welchen Voraussetzungen, welche Entscheidungsgrundlagen geschaffen werden können
- Risiken sollen umfassend analysiert werden. Dabei sollen Risiken betrachtet werden, die durch unzureichende Lenkungsmaßnahmen für die Gesellschaft entstehen können, genauso wie Risiken, die für Unternehmen durch den Zugriff auf ihre Daten entstehen können
- Evaluiert werden sollen die Potenziale von Verfahren zur vertraulichkeitsbewahrenden Analyse und Verarbeitung interner Daten (z.B. Verarbeitung und Analyse von verschlüsselten Daten, verteilte Verarbeitung und Analyse von Daten)

- Geklärt werden soll, welche Chancen und Gefahren jene Anwendungsfälle bergen, die ein Lagebild unabhängig von einer konkreten Krise erfordern; periodische Abfragen könnten vor allem im Hinblick auf die proaktive Vermeidung von Störungen bei der Versorgung hilfreich sein
- Untersucht werden soll, welche Anreize geschaffen werden müssen, um Unternehmen zu einer konstruktiven Mitwirkung zu bewegen; gesetzlicher Zwang zur Mitwirkung soll nach Möglichkeit vermieden werden
- Erörtert werden soll, wie sich eine geeignete Datenarchitektur erfolgreich aufbauen, einführen und betreiben lässt; in Frage kommt neben einem Aufbau und Betrieb durch die öffentliche Verwaltung auch ein privatwirtschaftliches Engagement
- Um die Umsetzbarkeit zu belegen und das Potenzial zu verdeutlichen, soll ein Demonstrator eine Beurteilung im Hinblick auf die Skalierbarkeit ermöglichen.

Eine enge Abstimmung mit dem KIRAS-Projekt DAGMAR wird vorausgesetzt, da in diesem Projekt die konzeptionellen Grundlagen für eine vereinheitlichte Datensammlung und -aufbereitung bereits gelegt werden.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.9 Intelligentes Meldungs- und Alarm-Management für Technisches Monitoring in kritischen Verkehrsinfrastrukturen

Kontakt: Bundesministerium für Klimaschutz, Umwelt, Energie. Mobilität, Innovation und Technologie (BMK)

E-Mail: andreas.herndler@bmk.gv.at

Kontakt: ASFINAG Maut Service GmbH, Christian Göltl, Abteilungsleiter IT Service Management (ASFINAG)
E-Mail: christian.goeltl@asfinag.at

Um einen effizienten und sicheren Betrieb des hochrangigen Straßennetzes sowie der besonders sicherheitskritischen Tunnel zu gewährleisten, ist der breite Einsatz von Überwachungs- und Steuerungsinfrastruktur (beispielsweise Verkehrs- und Umfeldsensoren, Wechselverkehrszeichen, Brandmelder, Notrufmelder, etc.) unerlässlich. Diese Überwachungs- und Steuerungsinfrastruktur stellt, nicht zuletzt durch ihre wechselseitigen Abhängigkeiten, selbst einen kritischen Faktor dar, deren ordnungsgemäße Funktionsweise durch entsprechendes technisches Monitoring sichergestellt werden muss.

Im Zuge des technischen Monitorings wird im Echtbetrieb eine Unmenge an isolierten Betriebs- und Überwachungsmeldungen sowie Alarmen, bei der ASFINAG österreichweit hunderttausende von Meldungen pro Tag, durch die unterschiedlichen Betriebsmittel der Überwachungs- und Steuerungsinfrastruktur

generiert. Diese müssen – so der Stand der Technik – durch die verantwortlichen Operator:innen in Verkehrsmanagementzentralen permanent bzgl. ihrer Relevanz überwacht und deren direkte und indirekte Auswirkungen auf den Betrieb interpretiert werden. Ziel des Verkehrsbetriebes ist es auf Basis dieser Meldungen zeitnah betrieblich adäquate Maßnahmen zu setzen.

Zusätzlich zu dieser Flut an Meldungen und Alarmen, stellen Eigenschaften der Überwachungs- und Steuerungsinfrastruktur selbst eine große Herausforderung für das technische Monitoring dar. Diese umfassen zum einen die Heterogenität innerhalb der Überwachungs- und Steuerungsinfrastruktur, die meist jahrzehntelang "gewachsene" Systeme unterschiedlichster Hersteller umfasst, wodurch sich Betriebsmittel, die darüber hinaus in unterschiedlichen Varianten und Versionen parallel im Einsatz sind, in ihrem Normal- und Fehler-Verhalten stark unterscheiden. Zum anderen sind die wechselseitigen Abhängigkeiten sowie die Größe der Überwachungs- und Steuerungsinfrastruktur und deren regionale Verteilung herausfordernd. Zu guter Letzt wird die Komplexität durch die omnipräsente dynamische Veränderung der Überwachungs- und Steuerungsinfrastruktur verstärkt, sowohl in Bezug auf geplante Veränderungen, z.B. aufgrund von Wartungsarbeiten, als auch hinsichtlich unvorhergesehener Veränderungen, z.B. in Form von Stör- und Fehlerfällen.

Im Hinblick auf diese großen Herausforderungen an das technische Monitoring gibt es derzeit keine hinreichende automatisierte Unterstützung für die verantwortlichen Operator:innen bei der Identifikation, Priorisierung und Interpretation relevanter Meldungen und Alarme sowie der Ableitung geeigneter Maßnahmen. So sind beispielsweise durch die nicht vernetzten Informationen über wechselseitigen Abhängigkeiten bei Stör- und Fehlerfällen eine Erkennung von Ursache und Wirkung aus praktischer Sicht erschwert und eine Ableitung von Maßnahmen komplex und zeitintensiv.

Betrachtet man darüberhinausgehend den existierenden Stand der Forschung im Bereich des technischen Monitorings im Allgemeinen und im Bereich des Meldungs- und Alarm-Managements im Speziellen, so ist unbestritten evident, dass relevante Methoden zur Erkennung von Ursache und Wirkung, wie beispielsweise Alarm-Korrelations-Erkennung und Root-Cause-Analysen, in existierenden Meldungs- u. Alarm-Management-Systemen nicht ausreichend unterstützt werden.

Aus praktischer ebenso wie aus wissenschaftlicher Sicht sind daher innovative und intelligente Ansätze und Techniken zur Reduzierung und Aufbereitung der Überwachungsmeldungen und Alarme (Filterung, Typisierung, Gruppierung, Aggregierung, Priorisierung) und automatisierten Interpretation (Korrelations-Erkennung, Root-Cause-Analyse, Impact-Analyse) notwendig, um die verantwortlichen Operator:innen bei der Identifikation komplexer Stör- und Fehlerfälle der Überwachungs- und Steuerungsinfrastruktur sowie in der Folge bei der Koordination entsprechender Maßnahmen bestmöglich zu unterstützen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Systematische Analyse von Meldungen und Alarmen, um deren Relevanz in quantitativer und qualitativer Hinsicht besser einschätzen zu können
- Evaluierung des Stands der Technik im Bereich Meldungs- und Alarm-Management (Standards, Best Practices, …), um Optimierungspotentiale zu identifizieren
- Entwicklung von Lösungen für die intelligente Reduzierung und Aufbereitung von Meldungen und Alarmen (Filterung, Typisierung, Gruppierung, Aggregierung, Priorisierung, …), um eine zielgerichtete Fokussierung des technischen Monitorings zu erreichen
- Entwurf von Konzepten für den Aufbau eines Domänenmodells, um insbesondere unterschiedliche Betriebsmittel, deren Logiken und wechselseitige Abhängigkeiten abzubilden, welche die Voraussetzung für ein intelligentes Meldungs- und Alarm-Management bilden
- Entwicklung von Ansätzen zur Empfehlung geeigneter Maßnahmen für Operator:innen beim Eintritt bestimmten Meldungs- bzw. Alarmkonstellationen
- Agile Entwicklung eines Proof-of-Concept Prototyps möglichst in der Systemumgebung der ASFINAG, um laufend zu den Forschungstätigkeiten die Machbarkeit der entwickelten Konzepte und Techniken zu demonstrieren
- Aufzeigen von Optionen zur Integration in bestehende Meldungs- und Alarm-Management-Systeme und Betriebsprozesse der ASFINAG, um die Voraussetzungen für eine Übernahme in den operativen Betrieb auszuloten.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.10 Neue Gefahren und Herausforderungen für die Stabilität des Gesundheitssystems in Österreich durch neu oder vermehrt auftretende Infektionskrankheiten und allergieauslösende Neobiota (z.B. vektorenübertragene Krankheiten, Zoonosen,…)

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: IXA7@gesundheitsministerium.gv.at

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)
E-Mail: karin.rainer@ages.at

Bezugnehmend auf z.B. Auftreten, Management und Systemeffekte neuer sowie wieder-auftretender vektorübertragener Krankheiten (endemisch/pandemisch), Zoonosen, sowie Auswirkungen von hoch-allergenen, invasiven Pflanzenarten muss eine solide Datenlage für Österreich erstellt werden, um frühzeitig auf Risiken und Bedrohungsszenarien für die Gesundheit und damit die Gesundheitsversorgung zu reagieren.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse und Management neu sowie vermehrt auftretender Gesundheitsrisiken durch bestehende wie invasive/neobiotische Vektoren der Übertragung von Infektionskrankheiten (z.B. Insekten, Wild- und Nagetiere, Vögel etc.) unter Berücksichtigung des One-Health-Ansatzes
- Monitoring und Überwachung von neu identifizierten Vektoren und Zusammenführung von Datenbanken und Informationsquellen sowie Identifikation von Risikogebieten. Weiterer Schwerpunkt ist die Entwicklung von Validierungs- und Qualitätssicherungswerkzeugen zur Erhebung diesbezüglicher Gesundheitsrisiken und zum nationalen sowie internationalen/grenzüberschreitenden Austausch von diesbezüglichen Daten, Informationen und Lösungsansätzen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.11 Surveillance und Gewährleistung von Trinkwasser-Sicherheit und Wasser-Qualität

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)
E-Mail: alois.leidwein@ages

Wasser begleitet den Menschen tagtäglich. Als wichtigstes Lebensmittel füllt es die Wasservorräte im Körper und versorgt ihn mit Mineralstoffen wie Magnesium, Calcium oder Natrium. Als Nutzwasser wird es im Haushalt oder am Arbeitsplatz verwendet, und an heißen Sommertagen dient es Mensch und Tier als Abkühlung. In Österreich kann Trinkwasser jederzeit in bester Qualität aus den Wasserleitungen entnommen werden, und auch Badegewässer weisen durchwegs höchste Qualität auf. Diese elementare Ressource gilt es umfassend zu schützen.

Der durch den Klimawandel bedingte globale Temperaturanstieg führt auch zur Erhöhung der Wassertemperaturen von Oberflächengewässern, was ein übermäßiges Wachstum von Mikroorganismen verursachen kann. Von speziellem Interesse werden die Cyanobakterien erachtet, die landläufig auch als Blaualgen bekannt sind. Eine Massenentwicklung dieser Mikroorganismen (oftmals als CHAB (cyanobacterial harmful algal bloom) abgekürzt) kann die Wasserqualität beeinträchtigen und die Nutzbarkeit des betreffenden Gewässers stark einschränken. Einige Cyanobakterien-Spezies werden mit der Produktion von Toxinen assoziiert, die für Mensch und Tier gesundheitsgefährdend sind. Die Symptome, die von diesen sogenannten Cyanotoxinen ausgelöst werden, sind vielfältig und reichen üblicherweise von Hautreaktionen, Entzündungen bis hin zu Magen- und Darminfektionen. Bei Tieren, speziell bei Hunden, kommt es jedoch auch gelegentlich zu Lähmungserscheinungen oder sogar zum Tod.

Eine weitere potenzielle Auswirkung des Klimawandels auf den Landschaftswasserhaushalt wurde kürzlich erst beschrieben. Durch den tendenziell

sinkenden Grundwasserstand drückt das Grundwasser anders als bisher an vielen Stellen nicht mehr nach oben und speist Oberflächengewässer wie Bäche und Flüsse (exfiltriert), sondern das Wasser der Fließgewässer versickert mehr in den Untergrund (infiltriert). Als Folge dieser Druckumkehr können mit den Oberflächengewässern auch Schadstoffe ins Grundwasser eindringen, das die wichtigste Trinkwasserquelle in Österreich darstellt.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

Um Wasser als qualitativ einwandfreie Ressource zu schützen, sollen in den Bereichen (Erholungs-/Nutz-) Gewässer und Trinkwasser folgende Forschungs-Schwerpunkte gesetzt werden:

- Sicherheit bei anhaltenden Effekten des Klimawandels z.B. bei Einbezug von Gefahren in Nutz- und Badegewässern durch Anstieg von Cyano-Bakterien etc.
- Nationale Beobachtung von neuen, klimatisch hervorgerufenen Gefahren für Trinkwasser sowie z.B. Microcystine in Wassertieren, die auch als Lebensmittel genutzt werden
- Sicherheit und Einbezug von Wasser-Qualitäts- und Prüfdaten in digitale Systeme z.B. zur Steigerung eines stabilen Austausches zwischen Wasser-Versorgern und Analyse-Organen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.12 Evidenzbasierte Governance-Plattform zur Entscheidungsfindung im Krisenmanagement

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)
E-Mail: alois.leidwein@ages.at

Für sämtliche Krisenfälle gilt, dass Entscheidungen meist unter unvollständigem Wissensstand und z.T. sehr schnell getroffen werden müssen. Das trifft auf spontan eintretende Szenarien – Naturkatastrophen, Terrorangriffe, hochinfektiöse Krankheiten – genauso zu wie auf sich schleichend entwickelnde Risiken – Klimawandel, politische, gesellschaftliche und demografische Entwicklungen, die immer wieder spontane „Eruptionen“ mit sich bringen. Zudem werden wir als Gesellschaft mit Herausforderungen zunehmender Komplexität konfrontiert („wicked problems“), die Notwendigkeit mit sich bringt, einen Handlungsauftrag umzusetzen, während gleichzeitig erst die für diesen Handlungsauftrag notwendige empirische Datengrundlage in Echtzeit aufgebaut werden muss. In die Prävention vor und / oder in die Abwehr von derartigen Situationen involvierte Organisationen stehen vor dem Dilemma, auf valide und zuverlässige Daten zurückgreifen zu

müssen, um sachgerechte Entscheidungen treffen zu können. Zudem sollte in diesen Fällen Wissen darüber bestehen, wer über welche Daten in welchem Umfang und welcher Granularität bereits verfügt, um Redundanzen und Ineffizienzen beim „Datenmanagement“ in akuten Fällen zu vermeiden.

Adressiert werden sollen Fragestellungen des Datenformats und der Aggregationsebene, Vorgehensweisen und Methoden zur Datensuche und -sammlung sowie des Aufbaus von Datenbanken, sowohl strukturell und hinsichtlich technischer Anforderungen, Verfahren zur Beurteilung der Datenqualität, aber auch Methoden, mit deren Hilfe sich die Bereitschaft zum Datenaustausch fördern lässt. Daten, die in Krisensituationen gebraucht werden, sollen für alle beteiligten Organisationen und rechtzeitig (so früh wie möglich) zur Verfügung stehen. Darüber hinaus sollen Fragestellungen rechtlicher und technischer Natur, wie zum Beispiel Datensicherheit, Zugriffsgewährung, Zugriffsgeschwindigkeit o. ä. eingeschlossen werden. Letztlich sind auch Fragen zu erörtert, wie eine solche Plattform als Teil eines Risiko-Governance-Mechanismus strukturell, organisatorisch und ressourcenmäßig effizient und effektiv aufgebaut werden muss.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können im Krisenfall relevante Akteure besser und schneller koordiniert werden, vor allem im Hinblick auf Wissensbedarf und Datenaustausch? Wie kann hierfür eine geeignete Plattform geschaffen werden?
- Wie kann in Krisensituationen eine verlässliche und schnell abrufbare Datengrundlage geschaffen werden, die hinsichtlich ihrer Zuverlässigkeit bewertet werden kann? Wie kann die Qualität der Daten im Hinblick auf Unsicherheit, Ambiguität, soziale Gerechtigkeit o. ä. beurteilt werden?
- Wie kann eine Vorgehensweise zur permanenten Überwachung von sensiblen Bereichen mit dem Ziel des Erkennens von „Emerging Risks“ geschaffen werden? Wie können Daten beurteilt werden, als Frühwarnindikatoren geeignet zu sein? Wie können bereits bestehende Instrumente mit dieser Zwecksetzung sowie deren Anwendbarkeit für Österreich beurteilt werden?
- Wie kann Datenmanagement zu einer verbesserten Risiko- und Krisenkommunikation beitragen, sowohl im Netzwerk zwischen den involvierten Akteuren als auch gegenüber der Öffentlichkeit?
- Entwicklung eines Konzeptes und AI unterstützten Demonstrators zur repetitiven Erfassung und Beschreibung von Bedarfen und Lösungen für das nationale Pandemie- und Katastrophenmanagement, das eine standardisierte Darstellung sowie einen Abgleich von Bedarf und Lösungen ermöglicht.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.13 Hitze und Unwetter als Risiko: Resilienz und Krisenfestigkeit des Gesundheitswesens sicherstellen

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: Manfred.Ditto@gesundheitsministerium.gv.at

Kontakt: Gesundheit Österreich GmbH (GÖG)
E-Mail: andrea.schmidt@goeg.at

Extrem hohe Temperaturen sowohl tagsüber als auch nachts sowie auch das vermehrte Auftreten von Hitzewellen zählen mit zu den markantesten Auswirkungen des Klimawandels. Laut der GeoSphere Austria ist eine Verdoppelung bis Verdreifachung der Hitzetage (Tagesmaximumtemperatur > 30 °C) in den österreichischen Landeshauptstädten zu erwarten. Die signifikante Zunahme der Hitzebelastung fordert die Gesundheit der gesamten Bevölkerung: vom Baby oder Kleinkind bis zum Erwachsenen, aber insbesondere vulnerable Bevölkerungsgruppen wie ältere und/oder pflegebedürftige Personen, Kinder insbesondere Säuglinge und Kleinkinder, schwangere Frauen, Personen mit chronischen Erkrankungen. Das hat auch Konsequenzen für das Gesundheitssystem auf unterschiedlichen Ebenen.

Zum einen ist mit einem erhöhten Versorgungsbedarf zu rechnen:

(1) Hitzebedingte Krankenhausaufenthalte und Todesfälle nehmen drastisch zu
(2) Heilungsprozesse werden potenziell verlangsamt. Durch die veränderte Wirksamkeit von Medikamenten sind auch Krankheiten ohne direkten Hitzebezug betroffen
(3) Pflegearbeit und -bedarf steigt, da besonders pflegebedürftige und vulnerable Gruppen an Hitzetagen mehr Betreuungsdienstleistungen in Anspruch nehmen.

Zugleich trifft die Versorgung auf neue Herausforderungen:

(1) Die Beschäftigten im Gesundheitswesen selbst sind durch Hitze geschwächt und bedürfen längerer Erholungszyklen, um produktiv arbeiten zu können
(2) Extremwetterereignisse und steigende Wahrscheinlichkeit für Jahrhundert-Hochwasser gefährden die Infrastruktur und Stromversorgung
(3) Stockende globale Lieferketten aufgrund von Extremwetterereignissen an Produktionsstandorten von Medikamenten gefährden die zeitgerechte Versorgung mit Medikamenten
(4) Die private Betroffenheit des Gesundheitspersonals durch Hitze und extremes Wetter kann zu einer Überforderung dieser führen und somit die Verfügbarkeit notwendigen Personals gefährden.

Hitze und Hitzewellen üben somit auf mehreren Ebenen einen nicht zu unterschätzenden Druck auf die Versorgungsstrukturen aus bzw. wird dieser durch die Kombination mit parallel auftretenden Ereignissen wie andere Extremwetterereignisse zusätzlich verstärkt. Es bedarf daher einer Stärkung des

Gesundheitssystems, um die Resilienz und Krisenfestigkeit zu sichern. Wesentlich ist hierfür ein umfassender Blick auf Infrastruktur, Personalbedarf, globale Auswirkungen der Klimakrise sowie mögliche Folgen für das Gesundheitssystem.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Systematische Erfassung und Analyse zu Hitzebelastungen und hitzebezogenen direkten und indirekten gesundheitlichen Folgen
- Identifikation von Resilienz-Szenarien für die Gesundheits- und Pflegeversorgung, die auch die Infrastruktur, den Personalbedarf und die globalen Auswirkungen der Klimakrise umfassen
- Ggf. Verschneidung mit (anderen) Krisenszenarien (z. B. gleichzeitiges Auftreten anderer Extremwetterereignisse sowie deren gesundheitlichen Folgen, paralleler Ausfall kritischer Infrastruktur) und deren Folgen für die Versorgungssicherheit
- Systematische Identifikation krisenanfälliger Regionen, Personengruppen sowie Versorgungseinheiten in Österreich
- Handlungsempfehlungen zur Weiterentwicklung von Hitzeschutz- und Hitzeaktionsplänen im Gesundheitswesen mit Fokus auf Beschäftigte im Gesundheitswesen aber auch pflegende Angehörige.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.14 Disaster Nursing - Sicherstellung von Pflege in Krisensituationen

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: katharina.meichenitsch@sozialministerium.at

Kontakt: Gesundheit Österreich GmbH (GÖG)
E-Mail: elisabeth.rappold@goeg.at

Sowohl die Covid-19 Pandemie als auch die alltägliche Berichterstattung zeigt, wie wichtig das Thema Katastrophenvorsorge inzwischen in allen Bereichen der Gesellschaft geworden ist. Übergreifend gilt es jedoch auch das Augenmerk auf jene Gruppen zu lenken, die hilfe- und pflegebedürftig sind sowie auf die unterschiedlichen Settings in denen alltäglich Pflegeleistungen erbracht werden.

Ca. 470.000 Personen sind in Österreich hilfe- und pflegebedürftig (Pflegegeldbezieher:innen lt. Statistik Austria 2022), mehr als 165.000 Personen in Pflegeberufen tätig und darüber hinaus engagieren sich noch rd. eine Million An- und Zugehörige im Bereich der informellen Pflege. In allen Settings, in denen Pflege geleistet wird, gilt es die zentralen Akteure ebenso wie die Organisationen selbst auf krisenhafte Situationen vorzubereiten und auszurichten, um im Krisenfall effizient handlungsfähig zu bleiben.

Das Gesundheits- und Sozialsystem in Österreich zeichnet sich durch Komplexität und Unübersichtlichkeit aus. Vielfach ist selbst den Akteuren im System nicht klar, wer, wann, wofür zuständig ist sowie wer welchen Bedarf mit welchen Mitteln und auf welcher Ebene beantworten kann. Die Unübersichtlichkeit und Zersplitterung von Aufgaben und Verantwortlichkeiten insbesondere in Krisen und Katastrophen stellt ein großes Risiko dar. Daher gilt es präventiv den Aufbau von Netzwerken und die Zusammenarbeit u.a. von Pflegediensten und Katastrophenschutz als eine Grundvoraussetzung für die erfolgreiche Bewältigung von zukünftigen Krisen und Katastrophen zu fördern und zu etablieren. Die dafür erforderlichen sektorenübergreifenden Maßnahmen stellen einen wesentlichen sicherheitspolitischen Beitrag dar.

Die Verfügbarkeit von organisatorischen Katastrophenschutzplänen in Organisationen und Diensten des Gesundheits- und Sozialwesens ist essenziell. Ihre Qualität wird auch maßgeblich davon beeinflusst, ob auch alle dafür relevanten Perspektiven eingeflossen sind – Konkret heißt dies, dass sie neben der Berücksichtigung von sicherheitspolitischen Aspekten, vor allem auf pflege- und gesundheitswissenschaftlicher Expertise einschließlich ethisch reflektierter Handlungsempfehlungen aufbauen.

Im internationalen Vergleich ist die systematische Auseinandersetzung mit den Herausforderungen im Bereich der Pflege in Notfällen, Krisen und Katastrophen - disaster nursing – in Österreich noch wenig entwickelt. Eine strukturelle Einbindung von Pflegeexpertise könnte mit der Entwicklung des Community Nursing erfolgen, erste Erfahrungen mit basaler Qualifizierung in diesem Bereich werden erst gesammelt. Eine wissenschaftlich fundierte konzeptionelle Grundlagenarbeit ist jedoch dringend erforderlich, um in weiterer Folge eine Agenda zu entwickeln, wie künftig eine widerstandsfähigere Pflege in relevanten Settings und damit auch mehr Sicherheit für alle Beteiligten vor, während und nach Notfällen, Krisen und Katastrophen gewährleistet werden kann.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation relevanter Handlungsfelder im Bereich der Pflege in Krisenzeiten, unter Berücksichtigung von Prävention, Förderung der Resilienz von professionell Pflegenden (Personen) sowie Organisationen (Mapping einschl. Erfassen der Perspektiven relevanter Expert:innen und Stakeholder)
- Recherche, Analyse und Darlegung des internationalen Forschungsstandes zur Vorsorge, Management und Bewältigung von Krisen und Katastrophen in unterschiedlichen Settings der Pflege
- Identifikation von zentralen Netzwerkpartnern in den unterschiedlichen Settings der Pflege in Krisen und Katastrophen und Entwicklung von Strukturen und Prozessen welche die Zusammenarbeit der Stakeholder fördern
- Analyse von Potenzialen, Entwicklungs- und Qualifizierungsbedarf der beruflichen Pflege im Bereich des Katastrophenmanagements unter Berücksichtigung der gesetzlichen Rahmenbedingungen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.15 Schutz kritischer Infrastruktur im Bereich AMR und Sicherstellung einer antimikrobiellen Therapie

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)

E-Mail: reinhild.strauss@gesundheitsministerium.gv.at

Antimikrobielle Resistenz (AMR) bedroht Gesundheit und Lebensqualität weltweit. Die Europäische Behörde für die Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen der Kommission (HERA) zählt AMR zu den drei größten Gesundheitsbedrohungen, die koordinierte Maßnahmen auf EU-Ebene im Zusammenhang mit medizinischen Gegenmaßnahmen erfordern. Der HERA-Vorstand hat eine Liste veröffentlicht, die drei Kategorien lebensbedrohlicher oder anderweitig ernsthaft bedrohlicher Gesundheitsgefahren enthält, die sich auf die Mitgliedstaaten ausbreiten können: 1) Krankheitserreger mit hohem Pandemiepotenzial, 2) chemische, biologische, radiologische und nukleare Bedrohungen und 3) Bedrohungen aufgrund antimikrobieller Resistenzen.

Durch Resistenzbildung können Infektionskrankheiten, die bisher gut durch antimikrobielle Mittel therapiert werden konnten, immer häufiger fatal enden. AMR und multiresistente Erreger führen zu erhöhter Morbidität und Mortalität, verlängerten Krankenhausaufenthalten und erhöhten Therapiekosten. Besonders immungeschwächte Personen in Alten-/Pflegeheimen, Neonatologien und Intensivstationen sind gefährdet. Durch vermehrte Personenmobilität (Globalisierung, Migration, Flucht) wird die Problematik verstärkt und resistente Keime nach Österreich gebracht. AMR stellt nicht nur ein Problem für einzelne Patient:innen dar, sondern durch Übertragungspotential und erhöhte Kosten/Personalressourcen auch für die öffentliche Gesundheit.

Die Gefahr eines Ausbruchs oder einer Verbreitung von (multi-)resistenten Erregern über nationale Grenzen hinweg stellt ein sicherheitspolitisches Risiko dar. Ein pandemisches Geschehen in Kombination mit antimikrobieller Resistenz bedeutet reduzierte Therapie- und Eindämmungsmöglichkeiten. Durch aktive Forschung, Entwicklung und Innovation soll eine kritische antimikrobielle Therapie für alle Patient:innen, die diese benötigen, gesichert und der Schutz kritischer Infrastruktur im Bereich AMR, speziell die medizinische Versorgung und der Zugang zu wirksamen Medikamenten und Therapieoptionen geschützt werden.

Ziel ist es, Forschung im Bereich der Prävention von AMR-Krisen zu fördern. Es soll der bisher wenig beachtete Bereich der antimikrobiellen Resistenz in Viren, Pilzen und Parasiten beleuchtet werden, schnelle Detektion von Resistenzen vorangetrieben und der Einfluss von Antiseptika (u.a. Desinfektionsmittel) auf AMR erforscht werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung von Antimikrobieller Resistenz in Viren, Pilzen und Parasiten
- Erforschung des Einflusses von Antiseptika auf AMR
- Erforschung von Rapid-Testing-Technologien in Bezug auf AMR.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.16 Innovatives Datenmanagement zur Bedarfs- und Distributionsplanung kritischer Medizintechnikprodukte in Krisensituationen

Kontakt: Land Steiermark, Abteilung 8 Gesundheit und Pflege (Land Steiermark)
E-Mail: abt08-cpid@stmk.gv.at

Die Gesundheitsversorgung ist eine der grundlegenden Säulen unserer Gesellschaft. Neben der Sicherheit im Gesundheitswesen (Arzneimittel, Medizinprodukte) sind Präventionsarbeit sowie Planung und Vorsorge zentrale Bestandteile dieses Bereichs.

Aktuell sind Gesundheitseinrichtungen dazu verpflichtet, Datenbanken zur Aufzeichnung und zur Verwaltung von Medizinprodukten und Geräten zu führen, welche in ihrem Verantwortungsbereich zur Behandlung von Patient*innen und zur Durchführung medizinischer Eingriffe im Einsatz stehen. Dies geschieht nahezu immer in lokalen und auf proprietären IT-Systemen aufbauenden Datenbanken. Durch die damit einhergehende Vielzahl unterschiedlicher Datenbanken und der auf sie zugreifenden Verwaltungssysteme ist es nicht möglich, einen Gesamtüberblick über die im Einsatz befindlichen oder die als strategische Reserve zur Verfügung stehenden Ressourcen zu bekommen. Somit stehen diese Informationen den Ländern, dem Bund oder auch anderen Bedarfsträgern für beispielsweise die Krisenvorsorgeplanung oder einer akuten Krisenbewältigung nicht oder nur sehr eingeschränkt zur Verfügung. Vor dem Hintergrund der gerade überstandenen Pandemie ist dies ein Zustand, den es zu überwinden gilt.

Der aktuell in Geltung stehende rechtliche Rahmen, das Medizinproduktegesetz (MPG) und die Medizinproduktebetreiberverordnung (MPBV), enthält bereits Regelungen über zu verwaltende Daten, legt die lokale Datenverwaltung in Krankenanstalten fest und würde dadurch auch die Grundlage für den Ansatz einer „Gesamtdatenbank“ bieten.

Durch die Schaffung einer einheitlichen, zentral verwalteten Plattform für Medizintechnik auf Basis lokal verwalteter Daten können Informationslücken geschlossen, Redundanzen verringert und Transparenz geschaffen werden. Damit wären unter Mithilfe von standortbezogenen Verknüpfungen aus GIS (Geo-Informations-Systemen) beispielsweise die Planung und die möglicherweise notwendige Verschiebung von kritischen Ressourcen im Krisenfall kurzfristig möglich. Ebenso würden sich neue Möglichkeiten bieten, die Resilienz von Krankenhausverbunden gegenüber Störungen des Regelbetriebs wesentlich zu steigern, da sich die Verlagerung und Distribution von Medizintechnik auch über Unternehmensgrenzen hinweg wesentlich effizienter gestalten ließe. So könnte zum Beispiel der dringende Bedarf an Beatmungsgeräten gleichen Typs und Herstellers in einer Abteilung eines anderen Krankenhausverbundes oder in einem anderen Bundesland vom System durch den Einsatz von Analyse-Routinen abgeklärt und bestenfalls zeitnahe adressiert werden. Gleichzeitig könnten verbleibende Versorgungskapazitäten neu berechnet und im System wieder als IST-Situation hinterlegt werden. Weiter könnten aus der vorhandenen einheitlichen Datenbasis über innovative Methoden wie dem Einsatz künstlicher Intelligenz (AI) wertvolle

Informationen über die Verfügbarkeit von, für spezielle Behandlungen oder zur Sicherung der medizinischen Grundversorgung unerlässlichen, Medizingeräten rasch aufgezeigt werden.

Unserer Ansicht nach ergibt sich daraus folgender Forschungsbedarf:

- Ermittlung der Datenlage sowie des derzeitig gelebten Datenmanagements in den unterschiedlichen Gesundheitseinrichtungen (z.B. Krankenhausverbunden) zur Erfüllung der Versorgungssicherheit -> Geospatial Knowledge Graph für Krankenhäuser und Medizingeräte
- Analyse von Methoden und Technologien zur Betreuung und Verwaltung der Datenbank und der Strukturebenen auf Bundes-, Landes bis hin zur Krankenhausebene
- Ermittlung der noch fehlenden legislativen Rahmenbedingungen zur möglichen Umsetzung einer solchen Datenbank unter besonderer Berücksichtigung des Datenschutzes
- Flexible und zuverlässige Erhebung und Extraktion von Daten zur Planung und Steuerung von medizinischen Ressourcen in der österreichischen Gesundheitslandschaft
- Entwicklung nutzerfreundlicher Interfaces („usage“ und „usability“) zur lokalen Datenpflege von Medizintechnik in einer Gesamtdatenbank
- Ableitung und Simulation von Szenarien für die Verteilung von Medizingeräten im Bedarfs- /Krisenfall
- Methodischer Ansatz zur Ableitung einer Risikomatrix aus der Datenbank zur raschen Beurteilung einzelner Medizinprodukte und deren möglicher Distribution an einen Bedarfs- /Krisenstandort
- Untersuchung der Potentiale und Möglichkeiten der Verknüpfung vorhandener Daten mit Geo- Informationen und zum Einsatz von AI-basierten Algorithmen.

Die Bearbeitung der vorgenannten Themenkomplexe und die dadurch zu erwartenden Erkenntnisse und Lösungen verfolgen das Ziel, den Herausforderungen und Gefahren betreffend die österreichische Gesundheitslandschaft zukünftig besser begegnen zu können.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.17 Austausch interoperabler Daten im Bereich Krisen- und Katastrophenmanagement

Kontakt: Das Land Steiermark, Fachabteilung Katastrophenschutz und Landesverteidigung (Land Steiermark)

E-Mail: Günter Hohenberger, MSc, katastrophenschutz@stmk.gv.at

Um tägliche Notfälle und größere Schadensereignisse erfolgreich bewältigen zu können, ist eine engmaschige Zusammenarbeit von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) unerlässlich. Grundlage für eine solche Kooperation

ist der effiziente und zeitnahe Austausch von Informationen, um ein möglichst vollständiges Lagebild ("Eigene Lage", "Schadens- und Gefahrenlage" und "Allgemeine Lage") zu erhalten. Diese Informationen können z.B. Standort-, Verfügbarkeits-, Dispositions- und Einsatzdaten umfassen, die entweder statisch (z.B. Adressdaten, Verkehrsnetze) in Echtzeit (z.B. bzgl. aktueller Aktivitäten) oder historisch (z.B. bzgl. Aktivitäten der Vergangenheit) übermittelt werden. Der erfolgreiche Austausch dieser Daten ist entscheidend für das Ableiten effizienter Maßnahmen und Entscheidungen. Viele BOS nutzen unterschiedliche Plattformen (z.B. Einsatzleitsysteme, Führungsinformationssysteme) und verarbeiten Informationen in verschiedenen Datenformaten, die intra- and interorganisationale Nutzung von Informationen erschweren und zu Lasten der Effektivität und Effizienz des gesamten Krisen- und Katastrophenmanagements ausfallen. Darüber hinaus können divergierende rechtliche Zuständigkeiten und Mandate den Austausch wertvoller Daten weiter behindern. Eine vielversprechende Lösung ist in der Weiterentwicklung von Data Spaces zu erwarten. Dabei handelt es sich um eine Kombination von technischen Komponenten und Vereinbarungen, die den Prozess des Austauschs sensibler und offener Daten, Services und Infrastrukturen definieren. Für den Austausch und die Nutzung der Daten werden im Vorfeld Bedingungen definiert, die sich z.B. an den rechtlichen Vorgaben für den Umgang mit hochsensiblen und privaten Daten (entweder organisations- oder personenbezogen) orientieren können. Auch zweckbezogene oder befristete Bedingungen bzgl. der ausschließlichen Nutzung der Daten für einen konkreten Einsatz sind möglich. So kann die Implementierung eines Data Spaces für BOS ein System zur Nutzung wertvoller Daten, Services und Infrastruktur bieten, das zudem die die geeigneten Mechanismen zur Handhabung sensibler Daten berücksichtigt. Der entstandene Datenraum soll ein solches System realisieren und zur stärkeren Interoperabilität und Resilienz von BOS für ein verbessertes Krisen- und Katastrophenmanagement beitragen.

Der Forschungsbedarf stellt sich folgendermaßen dar:

- Identifikation der Stakeholder und Klassifikation relevanter Akteure auf strategischer, operativer und taktischer Führungsebene, sowie deren potenzielles Datenangebot (als Datenlieferanten) und Informationsbedarf (als Datennutzer)
- Identifikation von Einsatztypen und Metriken, die aufgrund des verbesserten Datenangebots aus dem Data Space verbessert werden können
- Untersuchung bestehender Datenmodelle (z.B. EMSI), die im Kontext des Krisen- und Katastrophenmanagements verwendet werden können, sowie Entwurf neuartiger Datenmodelle, sollten die bestehenden Modelle nicht ausreichend geeignet sein
- Untersuchung der zu berücksichtigenden rechtlichen Aspekte und zu erwartende Konsequenzen durch relevante Legislation (z.B. Data Act, Data Governance Act)
- Entwurf einer für das Krisen- und Katastrophenmanagement zugeschnittenen Datenraumarchitektur, auf Basis bestehender Referenzarchitekturen (z.B. Gaia-X)

- Spezifizierung der "Governing Bodies" relevanter Stakeholder, die für den Betrieb und die Pflege der Datenräume verantwortlich sind, unter Berücksichtigung von Möglichkeiten zu Berücksichtigung neuer Geschäftsmodelle
- Festlegung von Datenmanagementverfahren, die die lokalen Datenschutzvorschriften und Sicherheitsaspekte berücksichtigen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.18 Entscheidungsunterstützung für Einsatzkräfte

Kontakt: ÖBFV Kompetenzzentrum für wissensbasierte Gefahrenabwehr: OBI d. Fd. Dipl. Ing. Gerald Czech (ÖBFV)
E-Mail: gerald.czech@feuerwehr.or.at

Die weitreichenden Transformationsprozesse in der Energiebereitstellung und -versorgung, dem Mobilitätssektor, der industriellen Fertigung, dem Wohnbau oder der Abfallwirtschaft, erfordern auch von Einsatzkräften eine schnelle und flexible Anpassung an geänderte Rahmenbedingungen. Im Falle eines Schadensereignisses wie beispielsweise bei einem größeren Austritt von Energieträgern wie Wasserstoff, LNG oder Ammoniak aber auch beim Brand von Fahrzeugen und Speicheranlagen mit Lithium-Ionen-Akkus müssen kritische Entscheidungen unter Zeitdruck getroffen werden. Dies stellt eine große Herausforderung für Einsatzkräfte als Entscheidungsträger:innen aber auch für alle am Prozess beteiligten Verantwortungsträger:innen dar. Vor allem dann, wenn nicht wie bei herkömmlichen Einsatzszenarien auf ein breites Erfahrungswissen zurückgegriffen werden kann. Der Ausbildungs- und Erfahrungshintergrund von Einsatzkräften („Operational Bias“) prägt auch die Entscheidungsfindung maßgeblich. Derzeit bauen viele Entscheidungsunterstützungssysteme auf dem bekannten „Regelkreis der Führung“ auf, welcher den Führungsvorgang abstrahiert und daher die Phase der Entscheidungsfindung nicht im Detail behandelt. Derzeitige Forschungen zur Zukunft der Stabsarbeit fordern auch die Weiterentwicklung des Führungssystems. Die genauen Mechanismen der Entscheidungsfindung und der Informationsverarbeitung spielen jedoch eine zentrale Rolle in der Entscheidungsunterstützung und sind derzeit nicht ausreichend untersucht. Eine digitale Entscheidungsunterstützung kann konkrete, nutzbringende Vorschläge nur dann machen, wenn diese Mechanismen verstanden und für die digitale Verarbeitung ausreichend exakt definiert sind. Vor allem vor dem Hintergrund der Implementierung von KI-Systemen in der Entscheidungsunterstützung ist ein Forschungsbedarf gegeben. Welche Methoden der modernen Entscheidungsunterstützung mit und ohne Einsatz von KI gibt es, welche Daten werden benötigt, um diese Methoden nutzbar zu machen, wie müssen diese Daten aufbereitet und zur Verfügung gestellt werden und welche technologieunterstützen Methoden sind, am besten geeignet, menschliche Entscheidungsprozesse im Kontext von Einsätzen zur Gefahrenabwehr zu ergänzen? Eine weitere Fragestellung ist, inwieweit sich unterschiedliche Maßnahmen zur

Eindämmung bzw. zur Beherrschung der Auswirkungen des Klimawandels auf Einsatzmethoden und Einsatzführung im Katastrophenfall auswirken.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Modelle der Entscheidungsfindung werden derzeit bei Einsatzkräften in der Gefahrenabwehr angewendet und wie werden mögliche geschlechterspezifische Unterschiede berücksichtigt?
- Welche derzeit vorhandenen Methoden der Entscheidungsunterstützung haben sich in unterschiedlichen Feldern als tauglich erwiesen?
- Wie können Entscheidungsträger:innen zum richtigen Zeitpunkt mit allen erforderlichen Informationen versorgt werden, jedoch ohne eine Informationsüberlastung zu verursachen?
- Wie müssen Informationen aufbereitet und dargestellt werden, um diese möglichst bedarfsorientiert, geschlechtergerecht und bruchfrei in Entscheidungsfindungsprozesse einfließen zu lassen?
- elche Rahmenbedingungen müssen erfüllt sein, um KI-Systeme im Rahmen der Entscheidungsunterstützung auf unterschiedlichen Entscheidungsebenen zu implementieren?
- Welche ethischen Fragestellungen sind für den Einsatz von Entscheidungsunterstützungssystemen auf KI-Basis zu beachten?
- Sind KI-Systeme in der Lage fehlendes Erfahrungswissen in spezifischen Handlungsfeldern (z.B. Problemstellungen im Zusammenhang mit der Energiewende) auszugleichen oder den Aufbau von Erfahrungswissen zu beschleunigen?
- Können KI-Systeme menschliches Erfahrungswissen lernen und für eine verbesserte Entscheidungsunterstützung in der Gefahrenabwehr anwenden?
- Wie kann der Stand der Forschung zu Teaming zwischen Menschen und Maschine (KI) auf Entscheidungsunterstützungssysteme übertragen werden?
- Wie kann das Vertrauen von Einsatzkräften in Entscheidungsunterstützungssysteme gefördert und gemessen werden?

Das auf der ÖBFV-Wissensdatenbank öffentlich zur Verfügung gestellte Wissen soll in die Projektbearbeitung miteinbezogen werden. Die am besten geeigneten Methoden der Entscheidungsunterstützung sollen mit dem im KIRAS Projekt B.PREPARED entstandenen Laborprototypen für ein Notfallplanungs- und Entscheidungshilfesystem für Unfälle mit Gefahrstoffen kompatibel werden, um so dessen Effektivität im Übungseinsatz mit Praktikern überprüfen und demonstrieren zu können. Die erforschten Methoden sollen die Grundlage für ein zukünftiges verbessertes Entscheidungsunterstützungssystem in der Gefahrenabwehr bilden.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.19 Klimaresilienz von grundwasserbasierten Wasserversorgungsanlagen in Österreich

Kontakt: Wasserwirtschaftliche Planung, Gruppe Wasser – Abt. Wasserwirtschaft, Amt der NÖ Landesregierung, St. Pölten
E-Mail: stefan.rakaseder@noel.gv.at

Kontakt: Wasserverband Südliches Wiener Becken, Bad Vöslau
E-Mail: Herr Ing. Wolfgang Hiltl, wlv@wlv-voeslau.at

Ein Großteil der Trinkwasserversorgung in Österreich erfolgt über die Entnahme von Grundwasser aus Brunnen in Tal- und Beckenlagen. Häufig weisen diese Grundwasserleiter eine hydraulische Anbindung an ein oder mehrere Oberflächengewässer auf oder werden maßgeblich über die flächige Grundwasserneubildung aus versickernden Niederschlägen gespeist. Auf Basis des prognostizierten Klimawandels ist mit einer Änderung der Abflussverhältnisse in Oberflächengewässern sowie zumindest in Ostösterreich einer Reduktion der Grundwasserneubildung bei gleichzeitiger Erhöhung der Grundwasserentnahmen zu rechnen.

Somit ergibt sich für die Wasserversorger die Notwendigkeit, Handlungsoptionen zu entwickeln, um die Versorgungssicherheit zu gewährleisten. Zu diesem Zweck können regionale instationäre Grundwassermodelle verwendet werden, mit denen die räumlichen Auswirkungen von geänderten Randbedingungen in Form von Szenariorechnungen ermittelt werden. Auf diese Weise werden mögliche Tiefenlagen von Grundwasserspiegellagen prognostiziert, die zu einem eingeschränkten Betrieb bzw. im Extremfall zur Abschaltung einer Trinkwasserversorgungsanlage führen können. Auf Basis der Szenarien können Gegenmaßnahmen als Entscheidungsgrundlagen entwickelt werden, um die Auswirkungen des Klimawandels auf den Grundwasserspiegel abzumildern. In diesem Zusammenhang sind die starken Einschränkungen durch die intensiven Nutzungen in den Tallandschaften in einem multikriteriellem Umfeld zu berücksichtigen.

Folgender Forschungsbedarf ergibt sich mit Bezug auf die Themenstellung:

- Verallgemeinerung von Kriterien, die auf eine Gefährdung des störungsfreien Betriebs einer Wasserversorgungsanlage hinweisen
  - Ableitung von Möglichkeiten zur Früherkennung
- Erstellen eines Ablaufplans zur Beurteilung der Klimaresilienz einer Trinkwassergewinnungsanlage
  - Festlegung eines Minimalkatalogs von zu untersuchenden Auswirkungen
- Zusammenstellung von Anforderungen an ein geeignetes Prognoseinstrument (Grundwassermodell)
- Entwicklung von Kriterien zur Bewertung von Handlungsoptionen / coping mechanisms
  - Optimierung von Maßnahmen nach mehreren Kriterien (multi-criteria analysis)

- Abstimmung von Handlungsempfehlungen mit ÖVGW Richtlinie W88 (Wassersicherheitsplanung in der Trinkwasserversorgung).

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.20 Schutz kritischer Infrastruktur allgemein

Hier können weiterhin alle kooperativen Projekte eingereicht werden, welche das Thema Schutz kritischer Infrastruktur treffen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.2 KIRAS. Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für F&E-Dienstleistungen

3.2.1 Verschwörungsnarrative und ihre „Attraktivität“ für die Generation 45+

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Verschwörungsnarrative bergen die Gefahr, nicht nur das Vertrauen in wissenschaftliche Erkenntnisse, sondern auch in demokratische Institutionen und Prozesse zu untergraben und in der Folge den gesellschaftlichen Zusammenhalt zu gefährden. Darüber hinaus werden in diesen Narrativen oftmals ausgewählte Personengruppen, insbesondere Minderheiten, für vermeintliche Missstände verantwortlich gemacht, was zu Diskriminierung, Stigmatisierung und sogar Gewalt gegen diese Gruppen führen kann. Die während der Pandemie verbreiteten antisemitischen Verschwörungsnarrative verdeutlichen diese problematische Entwicklung. Zudem konnte in den letzten Jahren beobachtet werden, dass terroristische Gewalt von Einzelpersonen verübt wurde, deren Denken massiv von Verschwörungsnarrativen beeinflusst war.

Trotz der zunehmenden Relevanz von Verschwörungsnarrativen in Österreich besteht zu ihnen und zu ihrer Verbreitung innerhalb der österreichischen Bevölkerung noch immer ein gravierender Mangel an gesicherten Erkenntnissen. Zudem fehlt es auch an Erkenntnissen hinsichtlich der hierzulande zentralen Akteure, die ihre eigenen oder von Dritten übernommene Verschwörungsnarrative über soziale Medien verbreiten, sowie zu dem von diesen ausgehenden Gefährdungspotenzial.

Um auf die Verbreitung von Verschwörungsnarrativen reagieren zu können, braucht es (i) die Erforschung jener individuellen und sozialen Faktoren, die die Menschen für Verschwörungsnarrative anfällig machen, (ii) die Analyse von Radikalisierungsverläufen in Bezug auf Verschwörungsnarrativen sowie (iii) die Entwicklung von gezielten Präventions- und Gegenmaßnahmen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Die über Covid-19 hinausgehende quantitative Erforschung der Verbreitung von Verschwörungsnarrativen innerhalb der österreichischen Bevölkerung sowie die Identifizierung individueller und sozialer Risikofaktoren, die Verschwörungsnarrative begünstigen
- Eine qualitative Untersuchung der Motive und Entwicklungsverläufe von Personen, deren Weltbild von Verschwörungstheorien geprägt war/ist sowie des Einflusses von Verschwörungsnarrative auf Einzelpersonen und deren soziales Umfeld
- Die Identifizierung der zentralen Akteure, Netzwerke und Plattformen in Bezug auf Verschwörungsnarrative sowie der aktuell dominierenden Verschwörungsnarrative und deren „Beweisführung“, um glaubhaft zu sein

- Untersuchung der Frage, was Verschwörungsnarrative gerade für diese Zielgruppe so attraktiv macht bzw. welche Funktion(en) Verschwörungsnarrative für Verschwörungsgläubige haben.

Untersuchung, ob, und wenn ja welche, Verschwörungsnarrative besonders verbreitet sind.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.2 Akzeptanz von intelligenten Überwachungs- und Identifikationssystemen im öffentlichen Raum

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Der rasche technische Fortschritt im Bereich intelligenter Überwachungs- und Identifikationstechnologien ermöglicht schnellere, genauere und kostengünstigere Lösungen, welche vor allem im öffentlichen Raum entscheidende strategische und taktische Vorteile für involvierte Behörden und Institutionen bringen könnten. In diesem Kontext wirft die zunehmende Verfügbarkeit von Biometrie, Big Data Processing, künstlicher Intelligenz und maschinellem Lernen jedoch auch Fragen hinsichtlich der gesellschaftlichen Akzeptanz von Systemen, die auf diese Technologien aufbauen, auf. Diese hängt von mehreren, sich gegenseitig beeinflussenden Faktoren ab, welche von BürgerInnen, Behörden und Einsatzkräften unterschiedlich wahrgenommen werden. Beispielsweise beeinflusst das subjektiv wahrgenommene Sicherheitsgefühl oder das subjektiv wahrgenommene Vertrauen in die korrekte Verwendung der erhobenen Daten in hohem Maße die Bereitschaft, intelligente Überwachungs- und Identifikationssysteme im öffentlichen Raum zu akzeptieren. Die Erhöhung gesellschaftlicher Akzeptanz kann nur gelingen, wenn diese Einflussfaktoren empirisch erhoben und analysiert werden, und darauf aufbauend konkrete, umsetzbare und effektive Handlungsempfehlungen abgeleitet werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erstellung angepasster Akzeptanzmodelle für intelligente Überwachungs- und Identifikationstechnologien im öffentlichen Raum
- Durchführung von Akzeptanz-Studien mit VertreterInnen der relevanten Zielgruppen (BürgerInnen, Einsatzkräfte, etc.)
- Ableitung von konkreten, durchführbaren und effektiven Handlungsempfehlungen zur Steigerung der Akzeptanz von intelligenten Überwachungs- und Identifikationssystemen:
  - Berücksichtigung von Vorbehalten und Informationsbedürfnissen der Zielgruppe
  - Anpassung von Technologiedesign
  - Gestaltung von Benutzerschnittstellen
  - Entwicklung effektiver Kommunikationsstrategien.

Generell: Einbeziehung der Perspektive der relevanten Stakeholder im gesamten Forschungsprozess.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.3 Entwicklung von Maßnahmen zur Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (RKE-Richtlinie 2022)

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Die nationalen kritischen Infrastrukturen bzw. Einrichtungen stellen einen besonders sensiblen Bereich in Europa dar. Aus diesem Grund wurde, basierend auf dem „European Programme of Critical Infrastructure Protection (EPCIP)“ aus 2008, das „Österreichische Programm zum Schutz kritischer Infrastrukturen“ etabliert und 2014 (APCIP, 2014) weiterentwickelt. Im Dezember 2022 beschloss das europäische Parlament die Richtlinie „Resilienz kritischer Einrichtungen (RKE-Richtlinie)“, die die bisherige Richtlinie aus 2008 zum Schutz kritischer Infrastrukturen bzw. Einrichtungen ersetzen wird. Ziel dieser Richtlinie ist die Gewährleistung der Erbringung von Diensten im Binnenmarkt, die für die Aufrechterhaltung essenzieller gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind und die Verbesserung der Resilienz dieser kritischen Einrichtungen.

In Artikel 10 der RKE-Richtlinie ist gefordert, dass Leitfäden und Methoden zur Umsetzung der Richtlinie zur Verfügung gestellt werden, die Resilienz der Organisationen durch Übungen überprüft wird und Beratungen und Schulungen für Personal kritischer Einrichtungen bereitgestellt werden sollen. Darüber hinaus sollen geeignete rechtskonforme Plattformen für den freiwilligen Informationsaustausch zwischen den kritischen Einrichtungen konzipiert und betrieben werden. Diese Maßnahmen sollen die Fähigkeit kritischer Einrichtungen fördern die Folgen von Sicherheitsvorfällen, die den Betrieb stören könnten, zu begrenzen, aufzufangen, zu bewältigen und die Wiederherstellung zu gewährleisten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können Leitfäden und Methoden zur Unterstützung der kritischen Einrichtungen gestaltet werden?
- Welche Formate (z.B. Übungen, etc.) eignen sich zur Überprüfung der Resilienz der kritischen Einrichtungen?
- Wie sollen geeignete Plattformen, die einen freiwilligen und rechtlich konformen Austausch von Informationen der kritischen Einrichtungen fördern, konzipiert und betrieben werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.4 Risikopotenzial und Kontextfaktoren von jugendlicher Delinquenz und Viktimisierung in Bezug auf familienbasierte Formen von Kriminalität mit spezieller Berücksichtigung von Tendenzen soziökonomischer Marginalisierung in Migrationspopulationen

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Im Bereich der kriminellen Netzwerke und organisierter Kriminalität in unterschiedlichen sozialen Milieus und Herkunftsgruppen bilden sich familiäre Verbindungen immer wieder als ein relevantes Strukturmerkmal ab. Zahlreiche Forschungsarbeiten zeigen, dass familienbasierte kriminelle Netzwerke für die Anwerbung von Mitgliedern für kriminelle Aktivitäten auf Familienangehörige zurückgreifen. Darüber hinaus zeigt sich, dass kriminelles Handeln und der soziale Umgang mit Regeln und Normen durch Sozialisation erlernt werden. Dies führt insbesondere in kriminellen Familien dazu, dass Regelbrüche bereits ab dem Kindesalter als Handlungsmöglichkeit internalisiert werden, die in Folge dissoziative Prozesse und soziale Schließung anstoßen können.

In besonderer Weise betroffen von befähigenden als auch einschränkenden familiären Beziehungen sind Menschen mit Migrationserfahrung, wenn mit der Migration zusammenhängende biographische Brüche zu sozio-ökonomischer, politischer und kultureller Ausgrenzung führen. Marginalisierungs- und Diskriminierungserfahrungen können dann die Abhängigkeit von familiären, verwandtschaftlichen Netzwerken erhöhen, und damit auch die Verstetigung dissoziativer Prozesse sowie intergenerative Transmission von Kriminalität in besonderer Weise begünstigen.

Intergenerative Transmission von Kriminalität, Delinquenz sowie von dissoziativen Einstellungen gegenüber institutionellen (rechtsstaatlichen) Normen und den Exekutivorganen kann unter anderem auch aus den Erfahrungen und Einstellungen der Jugendlichen interpretiert werden. Adoleszenz gilt als ein Schwellenzustand, wobei das Jugendalter als kritisch für die Identitätsfindung und Entwicklung von sozialer Zugehörigkeit gesehen wird. Soziale Umgebung, Anleitung an geltende Normen und Verantwortlichkeiten sind dabei besonders wichtig, und sind nicht zuletzt auch von familiären Ressourcen und Strukturen abhängig. Diese können darüber entscheiden, ob (gelegentliche) Delinquenz ein Zeichen von Autonomieaushandlungen und dem Austesten von Grenzen im Zuge des Erwachsenwerdens bleibt, oder zur Weichenstellung für die Verstetigung intergenerativer krimineller Karrieren wird (einschließlich z.B. der Entstehung pseudo-legaler Gerichtsbarkeit, systematischer Gewaltanwendung zur Durchsetzung der eigenen Machtposition, Ablehnung des staatlichen Gewaltmonopols etc.). Der Forschungsschwerpunkt soll daher aus den Erfahrungen und Einstellungen von Jugendlichen, als eine besonders vulnerable und für die Präventionsarbeit zentrale Bevölkerungsgruppe, dissoziative und kriminalistisch relevante Entwicklungen erkennen und für die strategische kriminalistische Analyse nutzbar machen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung der Erfahrungen von Jugendlichen im Alter von 13 – 17 Jahren mit Delinquenz und Viktimisierungserfahrungen mittels Vergleichsgruppenanalyse sowie Ausarbeitung statistischer Zusammenhänge zwischen sozialen Milieus, (vererbten) Bildungsbiografien, Geschlecht und Migrationserfahrung; insbesondere durch Untersuchung des Dunkelfelds, um Kriminalitätserfahrungen auf das soziale Umfeld zu beziehen, und Instanzen der Sozialisation in Bezug auf rechtsstaatliche Werte und Normen erkennen zu können
- Erkennen von dissoziativen Prozessen der Jugendlichen, einschließlich ihrer Einstellungen gegenüber gesellschaftlichen, demokratiepolitischen und rechtlichen Institutionen des Staates, etwa Ablehnung demokratischer Werte, gesellschaftlicher Institutionen, Segregations- und Extremismustendenzen, vor allem im Zusammenhang mit familienbasierten Bindungen und dahingehenden kriminellen Strukturen
- Weiterentwicklung effizienter Präventionsstrategien, sowohl im polizeilichen als auch im kommunalen Kontext, die auf einer empirisch fundierten Kenntnis der soziodemografischen bzw. sozioökonomischen Prämissen und Kontextfaktoren von Kriminalitätserfahrungen von Jugendlichen basieren, und auf Ansätze familienbasierter Delinquenz schließen lassen
- Entwicklung konkreter Handlungsansätze, die im Bereich des Community Policings, der Initiative „Gemeinsam Sicher“, zur Anwendung kommen. Das hat in enger Abstimmung mit polizeilichen, kommunalen und Akteur:innen aus dem Bereich der Sozialarbeit zu erfolgen.

Ausarbeitung weiterer konkreter Handlungsempfehlungen und Interaktionsmöglichkeiten für den Wirkungsbereich des BMI betreffend integrative und kriminalpräventive Maßnahmen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.5 Stärkung der Rechtssicherheit durch Vereinheitlichung der Anforderungen an die interprofessionelle Zusammenarbeit zwischen der Polizei und Dolmetscherinnen und Dolmetschern in der Kommunikationsüberwachung

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Strafverfolgungsbehörden arbeiten mit Audiodaten aufgrund von Maßnahmen aus der Kommunikationsüberwachung (KÜ). Bedingt durch die steigende Mobilität von (internationalen) Tätergruppen erfordert die Auswertung der Daten zunehmend die Zusammenarbeit zwischen Ermittlerinnen und Ermittler sowie Dolmetscherinnen und Dolmetschern, wenn die Audiodaten von Abhörmaßnahmen in anderen Sprachen als der deutschen vorhanden sind. Für Dolmetscherinnen und Dolmetscher bedeutet dies, dass neben den translatorischen Anforderungen auch nicht-translatorische Anforderungen zu erbringen sind. Wissenschaftliche Untersuchungen haben gezeigt, dass sich kriminalistisch-forensische Anforderungen an die

translatorische Arbeit ergeben, wenn die abgehörten Audiodaten für die Beweisermittlung erfasst, gefiltert und ausgewertet werden. Zudem ergeben sich während der Abhörtätigkeit forensische Anforderungen, wie die Verschriftlichung und Stimmenerkennung. Die Stimmenerkennung ist wesentlich, da so erst die Zuordnung von Aussagen zu konkreten Personen und Strafverfolgung ermöglicht wird.

Aktuell zeichnet sich ein uneinheitliches Bild in der Vorgehensweise von Dolmetscherinnen und Dolmetschern in der Kommunikationsüberwachung (KÜ) ab. Insbesondere hinsichtlich der Relevanz des ausgewählten Audiomaterials für die Verschriftlichungen und Verwendung im Verfahren, der Transparenz und Genauigkeit und damit der Glaubwürdigkeit im Hauptverfahren von Beweismitteln, welche aufgrund von KÜ-Maßnahmen entstehen, fehlen einheitliche Vorgaben. Fehlende einheitliche Vorgaben schaffen Unsicherheit in Hinblick auf die Verlässlichkeit der Übersetzungen, die als Beweismittel im Verfahren eingesetzt werden und können daher rechtliche Folgen nach sich ziehen. Zudem sind die Arbeitsprozesse weitgehend nicht formuliert und damit nicht transparent.

Es besteht daher ein Mangel an Rechtssicherheit für die Ermittlerinnen und Ermittler sowie Dolmetscherinnen und Dolmetscher. Die Rechtssicherheit von Angehörigen der Strafverfolgungsbehörden und Dolmetscherinnen und Dolmetschern, wie auch die rechtliche Einordnung von Straftatbeständen sowie das Rechtsgehör der betroffenen überwachten Personen hängt eng mit der Zusammenarbeit von Dolmetscherinnen und Dolmetschern sowie den jeweiligen ermittelnden Personen zusammen. Daher ist ein besonderes Augenmerk auf die translatorische Arbeit im Rahmen der Ermittlungstätigkeit zu legen.

Höhere Rechtssicherheit könnte durch klare und nachvollziehbare translatorische Arbeitsprozesse und Transparenz in der Zusammenarbeit erreicht werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhöhung der Rechtssicherheit in der Ermittlungsarbeit durch eine systematische Analyse von Best-Practice-Beispielen aus der KÜ
- Ausarbeitung von Empfehlungen für translatorische Arbeitsprozesse aufgrund von wissenschaftlich fundierten Erkenntnissen
- Stärkung der Verlässlichkeit von Beweismitteln in der KÜ durch Transparentmachung der Arbeitsschritte
- Aufwertung der Stellung von Dolmetscherinnen und Dolmetschern in der KÜ durch gezielte Schulung zur rechtlichen Einordnung von Tatbeständen sowie Steigerung der Zuhörkompetenz in der translatorischen Arbeit bei Abhörhandlungen, um die Stimmenerkennung zu optimieren
- Stärkung der interprofessionellen Zusammenarbeit zwischen Dolmetscherinnen und Dolmetschern sowie Ermittlerinnen und Ermittlern, um die Arbeitsprozesse transparenter zu gestalten.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.6 ABC-UAV-Freisetzung

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

UAVs können als Ausbringungsmittel für ABC-Gefahrstoffe in Form von Aerosolen eingesetzt werden. Ein Einsatz von MiniUAVs für Attentate ist dabei genauso denkbar, wie die großflächige Kontamination durch Einsatz von UAVs, welche wie zur Ausbringung von Pflanzenschutzmitteln und -düngern in der Land- und Forstwirtschaft eingesetzt werden. Die Freisetzung bzw. die Gefährdung wird dabei maßgeblich von UAV-spezifischen Faktoren wie unter anderem Typ und Größe des UAV, Payload, Flughöhe, Fluggeschwindigkeit, sprüheinrichtungsspezifischen Faktoren wie Düsenanordnung oder Ausbringungsleistung pro Zeiteinheit sowie von stoffspezifischen Faktoren wie Toxizität, Aerosolgrößenverteilung und weiterer physikalisch-chemischer Eigenschaften bestimmt und ist abhängig von externen Faktoren wie der aktuellen lokalen Wetterlage.

Um das Bedrohungspotential bzw. die Wirkungsvorhersagen solcher Freisetzungen im Vorhinein einschätzen zu können werden valide und robuste Modelle und Algorithmen benötigt. Damit soll einerseits ermöglicht werden im Anlassfall eine schnell verfügbare und akkurate Einschätzung der Gefährdungszone bereitzustellen und andererseits präventiv die Größenordnung von für einen Angriff nutzbaren UAVs abzuschätzen. Im Agrarbereich wird das als Wirksamkeitsanalyse von ausgebrachten Aerosolen bezeichnet. Diese Methoden müssen kompatibel mit den in Österreich eingeführten zivilen und militärischen (ABC)-Informationssystemen sein bzw. in diese integriert werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche unabhängigen Parameter wirken sich auf die Ausbringung von Aerosolen durch UAVs aus?
- Wie können die notwendigen Parametern aus bestehenden Sensoren/Beobachtungen bereitgestellt werden bzw. für welche Parameter existieren noch keine Sensoren/Eingabemöglichkeiten?
- Wie können diese Parameter in Modelle/Algorithmen umgesetzt werden um in Echtzeit Voraussagen zu treffen?
- Welche Parameter sind mindestens notwendig, um Vorhersagen treffen zu können?
- Welche Parameter können auch durch Annahmen ergänzt werden?
- Wie können diese Modelle/Algorithmen in bestehende zivile und militärische (ABC-)Informationssysteme eingebunden/integriert werden?
- Welche Parameter müssen experimentell ermittelt werden und wie können Modelle validiert werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.7 C-UAS Demonstrator

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Nach erfolgreichen Forschungsprojekten in KIRAS wie z. B. AMBOS, SILBOS, SCALA, … soll eine möglichst gemeinsame Realisierung bisheriger Projektergebnisse in einem verlegbar einsetzbaren Demonstrator System für den Schutz kritischer Infrastruktur (Objektschutz bzw. Bereichsschutz) erfolgen. Im Fokus steht die schnelle Integration von Komponenten niedriger TRL zu einem verwendungsfähigen System.

Projektziel ist die Schaffung eines Demonstrators aus bisherigen Projekten (=Hard – und Software inklusive Schulung) welcher nach Projektende dem BMLV überlassen wird und durch BMLV getestet und betrieben werden kann.

Der Demonstrator soll den Partnern nach Möglichkeit auch weiterhin zur Verfügung stehen und im Rahmen künftiger Forschungsprojekte unkompliziert erweitert werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können Ergebnisse unterschiedlicher Projekte der kooperativen F&E auf Demonstrator Niveau integriert werden
- Welche Schnittstellen sind erforderlich, um einerseits in bestehende Systeme integrierbar zu sein und andererseits für künftige Forschungsprojekte modular erweiterbar zu sein
- Wie wirkt sich die Verwendung von Forschungshardware im Betrieb aus
- Wie kann ein Demonstrator für den Übungseinsatz gehärtet werden
- Wie kann ein Demonstrator im Experimentalbetrieb in Übungsszenarien integriert werden
- Wie kann eine Anwendereinschulung am Forschungsdemonstrator erfolgen
- Was muss bei einer Nutzung von Systemen mit niedrigen TRL berücksichtigt werden.

Wichtig ist hierbei, bestehende Ergebnisse laufender oder bereits abgeschlossener KIRAS- Projekte zu berücksichtigen und vorhandene Synergien und Ergebnisse zu nutzen. Eine Zusammenarbeit mit dem BMLV ist für den Projekterfolg notwendig. Um einen erfolgreichen Projektantrag zu gewährleisten, wird ersucht einen zweiten, zivilen Bedarfsträger (z.B. BMI) mit hinzuzunehmen, um den Dual-Use-Apekt zu unterstreichen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.8 Hochwasser- und Energieversorgungssicherheit an größeren Flüssen mit intensiver Wasserkraftnutzung im Spannungsfeld nutzungsbeeinflusster Sohlveränderungen und deren Auswirkung auf die Wassersversorgungs-sicherheit unter Berücksichtigung von Einflüssen des Klimawandels

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abt. I/4 – Anlagenbezogene Wasserwirtschaft (BML)
E-Mail: herbert.heindl@bml.gv.at ; Abt-14@bml.gv.at

Flusskraftwerke stellen ein zentrales Element für die Energieinfrastruktur in Österreich dar. Lauf-Wasserkraftwerke tragen zu ca. 36% zur heimischen Strombereitstellung bei (Stand 2021).

Dieser unverzichtbare Anteil an erneuerbarer Energieerzeugung (Versorgungssicherheit) steht im Spannungsfeld mit dem Schutzbedürfnis vor Hochwässern (Hochwassersicherheit), der Sicherung der Wasserqualität/-quantität von Oberflächen- und Grundwasser, dem Natur-/Umweltschutz etc. Zur langfristigen Erhaltung der ökologischen Funktionsfähigkeit der Flusssysteme für künftige Generationen gilt es nachhaltige Lösungsansätze zu entwickeln, um ein „ausbalanciertes" Gesamtsystem in Zeiten des Klimawandels zu erhalten und weiterentwickeln zu können.

Aufgrund der Reduzierung der Fließgeschwindigkeiten durch die Stauräume der Kraftwerke kommt es zur dortigen Ablagerung von Feinsedimenten, die im Falle größerer Hochwässer konzentriert weitertransportiert werden (durch die Staulegung i. S. der Hochwassersicherheit). Nach Wellendurchgang erfolgt die erneute Ablagerung der Sedimente, die dort zu unterschiedlichen Problemen führen können. Grobes Geschiebe wird meist an den obersten Stufen (Kopfstufen) bzw. den Zubringereinmündungen zurückgehalten bzw. entfernt, um die Hochwassersicherheit (Freiborde) nicht einzuschränken. Weiter flussabwärts entstehen durch den Rückhalt bzw. mangelnden Nachschub an grobem Sohlmaterial Defizitbereiche (oberhalb der Stauwurzelbereiche und in freien Fließstrecken) bzw. zu größeren Feinsedimentablagerungen in den Stauräumen. In den Stauräumen strebt die Sohle einen „neuen" Ausgleichszustand an, in freien Fließstrecken besteht durch mangelnden Geschiebenachschub ein Defizit an stabilisierendem Sohlmaterial. Seitenerosion ist durch historische Lauf-Begradigungen und Ufersicherungen nicht oder nur eingeschränkt möglich. Kurz und mittelfristig kann durch Gerinne-Aufweitungen, Uferrückbauten oder technische Geschiebezugabe (Rückführung bzw. Zugabe von nicht direkt flussbürtigem Material) Eintiefungstendenzen entgegengewirkt werden; Defizite durch Ablagerungen werden z.T. technisch durch Baggerungen/Spülungen entfernt. Absinkende Wasserspiegellagen haben absinkende Wasser-/Grundwasserspiegellagen zur Folge - mit möglichen Auswirkungen auf die Versorgungssicherheit (Landwirtschaft, Wasserversorgung, Schifffahrt etc.).

Nachhaltige, langfristig umsetzbare Lösungsansätze mit der Betrachtung des Gesamtsystems von ganz „oben" (Wildbach) bis ganz „unten" (Mündung Meer) liegen derzeit nicht vor bzw. bestehen große Herausforderungen.

Hochwasserentlastungen (die Wehranlagen) von Flusskraftwerken sind auf extreme Abflüsse ausgelegt, die auf einer Hochrechnung von Wasserstands- bzw. Durchflussmessungen beruhen. Diese sind im Allgemeinen mit Unsicherheiten behaftet und gehen im Wesentlichen davon aus, dass die Durchflüsse in unseren Flüssen sich in Zukunft ähnlich verhalten werden wie in der Vergangenheit.

Die Beobachtung größerer Hochwässer der jüngsten Vergangenheit machen eine Anpassung der damaligen „Bemessungswerte" erforderlich, wodurch eine Adaptierung der Nachweise bzw. u. U. ein Umbau der Wehr-Anlage erforderlich werden, um die geforderten Sicherheiten einzuhalten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Ist eine langfristige Lösung der Thematik i. S. eines morphologisch veränderlichen Systems (Erosion/Ablagerung - Ausgleichsbestreben) realistisch?
- Wie könnten angepasste/adaptive Lösungsansätze aussehen? Können Sohl-Eintiefungen in freien Fließstrecken dauerhaft mit verhältnismäßigem Aufwand verhindert werden?
- Ist eine Geschiebedurchgängigkeit durch Umbauten an den Wehranlagen technisch möglich/sinnvoll? Bevorzugte Anlagentypen?
- Kann die Hochwassersicherheit der Kraftwerksanlage dabei mit verhältnismäßigem Aufwand erhalten oder verbessert werden? Nachweisführung?
- Wie unterscheidet sich das Prozessverständnis hinsichtlich Geschiebe und Feinsediment? Müssen dahingehend kombinierte Ansätze entwickelt werden?
- zeitgemäße Modell-/Berechnungsansätze?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.9 Effiziente Frühwarn- und Alarmsysteme bei Störfällen an Stauanlagen

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abt. I/4 – Anlagenbezogene Wasserwirtschaft (BML)
E-Mail: burkhard.ruedisser@bml.gv.at

Stauanlagen sind die zentralen Elemente der Energieinfrastruktur in Österreich. Aufgrund ihrer Größe und der Menge an gespeicherter Energie beinhalten sie ein großes Gefährdungspotential im Falle einer Zerstörung.

Vor dem Hintergrund der Zerstörung des Kachowka-Staudammes in der Ukraine im Juni 2023 und der damit einhergehenden katastrophalen Überflutung der Unterliegergebiete mit zahlreichen Todesopfern und noch nicht absehbaren Auswirkungen auf die Umwelt, zeigt sich auch deutlich die mögliche Gefahr eines terroristischen Angriffes auf kritische Infrastruktur. Ein drohender Sabotageakt an einer Stauanlage kann durch herkömmliche Überwachungssysteme oft nur schwer im Vorfeld erkannt werden. Die Vorwarnzeiten für die Umsetzung der Alarm- bzw. Einsatzpläne zur Evakuierung der betroffenen Bevölkerung sind daher entsprechend kurz.

Frühwarn- und Alarmsysteme bei Stauanlagen sind wichtige Instrumente zur Gewährleistung der Anlagensicherheit. Sie dienen dazu, mögliche Störfälle oder Sabotageakte frühzeitig zu erkennen und angemessene Maßnahmen zu ergreifen, um Schäden zu verhindern bzw. Sicherungs- und Evakuierungsmaßnahmen einzuleiten. Diese Systeme überwachen unterschiedliche Parameter der Stauanlage selbst sowie ihrer Umgebung.

Wenn eine Gefahr als solche erkannt wird, sollen Frühwarn- und Alarmsysteme automatisch einen Alarm auslösen und die Aktivierung der bereits vorbereiteten Alarm- bzw. Einsatzpläne einleiten. Die Vorwarnzeit für die Bevölkerung bzw. die Effizienz der Alarm- und Einsatzpläne hängen dabei in einem entscheidenden Maß von Reaktionszeit des Frühwarn- und Alarmsystems sowie von der schnellen und zielgerichteten Umsetzung der Alarmierung ab.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche technischen und organisatorischen Lösungen von Frühwarn- und Alarmsystemen gibt es für Stauanlagen?
- Welchen Einfluss hat die Vorwarnzeit auf die Umsetzung der Alarm- bzw. Einsatzpläne sowie auf die möglichen Konsequenzen bei einem Störfall an einer Stauanlage?
- Bei welchen Stauanlagentypen bzw. Randbedingungen sind Frühwarn- und Alarmsysteme besonders effizient?
- Wie können bestehende Frühwarn- und Alarmsysteme optimiert werden, um dadurch die Vorwarnzeiten für die betroffene Bevölkerung zu verlängern?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.10 Aufbau und Betrieb eines flächendeckenden Prognose- und Detektions- und Alarmierungssystems in ständiger Bereitschaft für Waldbrände in Österreich (BML)

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abt. III/4 – Wildbach- und Lawinenverbauung und Schutzwaldpolitik, DI Kilian Heil
E-Mail: kilian.heil@bml.gv.at

Aufbau und Betrieb eines flächendeckenden Prognose- und Detektions- und Alarmierungssystems in ständiger Bereitschaft für Waldbrände in Österreich.

Im Hinblick auf die erwarteten klimatischen Veränderungen und die zunehmende sozioökonomische Nutzung des Waldes ist mit einem Anstieg der Waldbrandgefahr und eindringlicheren Folgen von Bränden in Österreich zu rechnen. Kaskadenartigen Auswirkungen auf das Ökosystem Wald und auf den Schutz der Bevölkerung (z.B. hinsichtlich Objektschutzwald) sind zu erwarten. Für ein integriertes Risikomanagement ist eine flächendeckende und systematische Anwendung von Prognose, Detektion und Alarmierung notwendig. Das entwickelte Konzept unterstützt die Maßnahmen zur Waldbrandbekämpfung, die eine herausfordernde aber notwendige Aufgabe im Dienst der Sicherheit der österreichischen Bevölkerung darstellen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Konzeptionierung von Verfahren und Systemen zur Vorhersage und Frühwarnung von Waldbränden
- Ermittlung des State-of-the-Art von flexibel einsetzbarer und störungsresistenter Sensorik zur Waldbranddetektion
- Erhebung von Energieversorgungskonzepten für nachhaltige Verwendung im Einsatzgebiet
- Entwicklung von automatisierten, flächendeckenden Monitoring-Systemen mit Hilfe von Fernerkundungsmethoden
- Automatisierte aussagekräftige Alarmierung um die Zeit bis zum schlagkräftigen Erstangriff verkürzen
- Sicherstellung der praktischen Anwendbarkeit methodischer Neuentwicklungen
- Transdisziplinäre Evaluierung der Prognose-, Detektions- und Alarmierungssysteme zwischen regionalen und lokalen Bedarfsträgern (Landeswarnzentrale, Feuerwehr) und der technisch-inhaltlichen Umsetzung;
- Untersuchung der Möglichkeiten einer vollständigen Integration in die Informationssysteme der Bundesländer, insbesondere der Landeswarnzentralen
- Schutzkonzepte für das Wildlife-Urban-Interface (WUI)
- Folgenabschätzungen welche Maßnahmen erforderlich sind, und welche Auswirkungen die vorgeschlagenen Lösungen hätten.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.11 Organisierte Kriminalität als Herausforderung für den Strafvollzug

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at , cc: andreas.bednarek@bmj.gv.at

Kriminelle Organisationen wirken auf verschiedene Arten auf das Strafvollzugssystem ein und machen zur Aufrechterhaltung der Sicherheit in Haft entsprechendes staatliches Handeln erforderlich, sowohl hinsichtlich der Verhinderung der Rekrutierung neuer Mitglieder, der Weiterführung krimineller Aktivitäten (speziell bei Personen, die in der Organisation führend tätig sind) als auch der Bildung neuer Gruppierungen. Internationale Forschung zeigt, dass die Inhaftierung von Angehörigen krimineller Organisationen zu einem Anstieg gewalttätiger Auseinandersetzungen führen kann, sowie zu einer Steigerung krimineller Aktivitäten wie Suchtgifthandel, Schutzgelderpressungen oder illegalem Glücksspiel. Zudem geht von den betroffenen Personen ein erhöhtes Risiko für weitere Straftaten nach der Entlassung aus.

Im internationalen Recht finden sich nur eklektische Anknüpfungspunkte für den Umgang mit dieser Thematik, bspw. im Rahmen der United Nations Convention against Transnational Organized Crime. Speziell hinsichtlich der Ausgestaltungsmöglichkeiten des Vollzuges liegen darüber hinaus vereinzelt internationale Richtlinien sowie Judikate des EGMR vor, die Anhaltspunkte für den

schwierigen Ausgleich zwischen sicherheitsbedingt notwendigen Beschränkungen einerseits und den Rechten der Insass:innen andererseits bieten, bspw. hinsichtlich einer Unterbringung in Einzelhaft oder einer Einschränkung der Außenkontakte.

Während das Thema in der internationalen Fachliteratur für verschiedene Jurisdiktionen teilweise behandelt wird, liegen hinsichtlich des österreichischen Strafvollzugs, soweit bekannt, keinerlei Untersuchungen vor, die sich mit der Frage der Existenz, Prävention und Bekämpfung von Organisierter Kriminalität in den österreichischen Haftanstalten befassen. Eine solche Untersuchung ist daher für die österreichischen Sicherheits- und Vollzugsbehörden von großer Bedeutung.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Sammlung, Sichtung und Analyse verbindlicher internationaler Vorgaben sowie Entscheidungen des EGMR zur Frage der Ausgestaltung von Haftbedingungen für Mitglieder der Organisierten Kriminalität
- Erhebung, Zusammenführung und Analyse des internationalrechtlichen Schrifttums und Erfahrungsschatzes zum Umgang mit Organisierter Kriminalität in Haft
- Untersuchung von Umfang und Ausprägung der Problematik sowie deren Handhabung im österreichischen Strafvollzug, inkl. Identifikation von Optimierungspotenzialen
- Erarbeitung von Best-practice-Guidelines zum Umgang mit dem Phänomen Organisierter Kriminalität in Haft.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.12 Fremdenrecht und Strafrecht – Schnittpunkte und wechselseitige Abhängigkeiten

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at , cc: andreas.bednarek@bmj.gv.at

Für den Vollzug des Fremdenrechts sind Verwaltungsbehörden bzw. Verwaltungsgerichte zuständig, für die Berücksichtigung fremdenrechtlicher Aspekte im Rahmen der Strafzumessung die Gerichte. Die mitunter lange Verfahrensdauer im Bereich des Fremdenrechts kann dazu führen, dass fremdenrechtliche Entscheidungen und Reaktionen erst lange nach den strafrechtlichen Maßnahmen erfolgen und bspw. auch fremdenrechtliche Freiheitseingriffe zeitlich nach strafrechtlichen Freiheitseingriffen gesetzt werden. Umgekehrt können fremdenrechtliche Maßnahmen Strafverfahren erschweren, wenn beispielsweise wichtige Zeug:innen (etwa in Verfahren wegen Menschenhandel oder Schlepperei) infolge eines fehlenden Aufenthaltsstatus rasch abgeschoben werden und im Strafprozess nicht mehr zur Verfügung stehen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Worin liegen die Interdependenzen zwischen Straf- und Fremdenrecht?
- Wie beeinflussen strafrechtliche Entscheidungen die fremdenrechtliche Entscheidung?
- Wie beeinflussen fremdenrechtliche Aspekte strafgerichtliche Entscheidungen und allfällige strafrechtliche Reaktionen?
- Inwieweit dürfen fremdenrechtliche Gesichtspunkte bei den strafrechtlichen Reaktionen berücksichtigt werden?
- Wie kann die Kooperation zwischen Straf- und Fremdenrecht vertieft werden, um Abschiebungen direkt aus der Strafhaft durchführen zu können, ohne zusätzlich eine Schubhaft zu benötigen?
- Wie können die Interessen der Strafrechtspflege und der notwendige Vollzug fremdenrechtlicher Entscheidungen bestmöglich in Einklang gebracht werden, um beispielsweise durch die Abschiebung wichtiger Zeug:innen nicht die zentralen Beweismittel für das Strafverfahren zu verlieren?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.13 Haftgestaltung für Frauen und Jugendliche durch sicherheitsarchitektonische Elemente

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at , cc: andreas.bednarek@bmj.gv.at

Die bauliche Gestaltung der österreichischen Justizanstalten, wie auch die organisatorischen und technischen Gegebenheiten, spielen eine entscheidende Rolle für die Sicherheit und die Umsetzung von Maßnahmen zur Reintegration Jugendlicher, wie auch weiblicher Insassinnen im Strafvollzug. Die große Anzahl erwachsener männlicher Insassen hat dazu beigetragen, dass es bisher nur wenig nationale und internationale Forschung zu diesen Themenfeldern gibt. Darüber hinaus haben sehr heterogene Haftbedingungen, aufgrund der Diversität der österreichischen Justizanstalten, dazu geführt, dass bisher keine einheitlichen baulichen Standards für diese Insass:innen etabliert werden konnten.

Aus diesen Gründen besteht dringender Forschungsbedarf die spezifischen Anforderungen dieser marginalisierten Gruppen und die bestehenden baulichen Gegebenheiten ihrer Unterbringung im österreichischen Vollzug zu untersuchen, um entsprechende Standards für deren bauliche Haftgestaltung entwickeln zu können. Zuerst soll der Status Quo der strukturellen, baulichen Gegebenheiten der Unterbringung, sowie organisatorischen und technischen Anforderungen von Jugendlichen und Frauen in Haftanstalten, unter besonderer Berücksichtigung entwicklungsbedingter Erkenntnisse und mittels einer geschlechtersensiblen Vorgehensweise, erhoben werden. Hierbei soll auf bisherigen Erkenntnissen aus relevanten laufenden und abgeschlossenen nationalen Projekten zu diesen Themenfeldern aufgebaut werden. Durch diesen Forschungsschwerpunkt soll evidenzbasiertes Wissen über die baulich relevanten Bedürfnisse von Frauen und Jugendlichen im Strafvollzug gewonnen werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Die psychische und physische Gesundheit von Insass:innen soll durch die Gestaltung der Haftumgebung unterstützt werden. Untersuchungen über die Auswirkungen des Umfelds auf das Wohlergehen der Insass:innen sind notwendig, um Maßnahmen zur Verbesserung der baulichen Haftbedingungen zu entwickeln. Frauen sollen dabei nicht auf gesellschaftlich tradierte Rollen festgelegt werden, sondern unterstützt werden selbstbestimmte Entscheidungen treffen zu können, die die Vereinbarkeit von persönlichen Wünschen und Bedürfnissen und die eventuelle Betreuung von Kindern zu ermöglichen. Jugendliche sollen in Ihrer Entwicklung zu selbstbestimmten und verantwortungsbewussten Erwachsenen gefördert werden. Bauliche Rahmenbedingungen sollen auf diese Bedürfnisse abgestimmt sein und die Justizwachbediensteten unterstützen die Vollzugsziele zu erreichen
- Einen wichtigen Aspekt bei der Haftgestaltung stellen angemessene Sicherheitsstandards dar. Hierbei soll auf eine Vereinbarkeit von Privatsphäre und Sicherheit Wert gelegt werden. Weitere Forschungsarbeiten sind erforderlich, um gendersensible und dem jungen Erwachsenenleben angepasste Sicherheitsstandards zu definieren und dadurch den männlich geprägten Strafvollzug zu ergänzen
- Die strukturelle Gestaltung der Justizanstalten ist auf die Förderung der Reintegration von Frauen und Jugendlichen auszurichten. Es bedarf der Durchführung entsprechender Analysen, um bauliche, wie sozial-organisatorische Aspekte zu erarbeiten, die eine erfolgreiche Wiedereingliederung von Frauen und Jugendlichen in die Gesellschaft zu ermöglichen
- Zur Erarbeitung von Konzepten für die baulich-strukturelle Gestaltung von Frauen und Jugendlichen in Haft sind internationale Best-Practice-Beispiele heranzuziehen. Darüber hinaus sollen Erkenntnisse nationaler und internationaler Studien für den österreichischen Strafvollzug analysiert werden, um wirksame Maßnahmen entwickeln zu können.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.14 Konzeptuelle Weiterentwicklung des Konzepts der wirtschaftlichen Landesverteidigung in einem europäischen Kontext

Kontakt: Bundesministerium für Arbeit und Wirtschaft, Sektion VI – Nationale Marktstrategien, Referat VI/9a – Krisenmanagement, Ing. Mag. Michael Stern (BMAW)
E-Mail: michael.stern@bmaw.gv.at

Die zuletzt durchlaufenen Krisen, wie die Covid-19-Pandemie, den Russland-Ukraine-Konflikt sowie die damit einhergehende Energiekrise, aber auch die Evergreen-Havarie im Suezkanal verdeutlichen einerseits die ganz konkret erlebbaren wirtschaftlichen Konsequenzen derartiger Krisen aber auch deren multiplen und

komplexen Charakter sowie die Kaskadeneffekte für die österreichische Wirtschaft in einem europäischen Kontext. Zusätzlich bewirken der Klimawandel und die Digitalisierung die Beschleunigung neuer Technologie-Entwicklung mit breitem Anwendungsfokus (Elektromobilität in der Fahrzeugindustrie, Photovoltaik, Batterie-Technologien, Mikrochips) und damit auch Bedarf an bestimmten Rohstoffen oder Technologien, die in der Welt geographisch ungleich verteilt sind. Dies führt auch zu einer geopolitischen Dynamik, der sich Staat, Wirtschaft und Gesellschaft konfrontiert sieht.

Der bisherige Begriff der wirtschaftlichen Landesverteidigung soll in diesem Kontext zu einem modernen österreichischen Wirtschaftsschutzkonzept im europäischen Kontext weiterentwickelt werden, um die Resilienzfähigkeit der österreichischen Wirtschaft unter Berücksichtigung ihrer strukturellen Spezifika zu optimieren.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse der aktuellen Bestrebungen und dem Reifegrad zur wirtschaftlichen Landesverteidigung bei europäischen Partnern.
- Identifikation und Kategorisierung von spezifischen Verwundbarkeiten und externen Abhängigkeiten im österreichischen Wirtschaftsraum unter Berücksichtigung seines signifikanten Anteils an Klein- und Mittelbetrieben sowie externen Wirtschaftsbeziehungen, etwa spezifische Rohstoffe, Technologien, Vorprodukte, Güter und Knowhow
- Spezielle Berücksichtigung der Verwundbarkeiten und Abhängigkeiten bei kritischen Infrastrukturservices, wie insbesondere Informations- und Kommunikationstechnologie (IKT) inklusive Cybersecurity, Energie, Transport und Logistik
- Diskussion der Akteurslandschaft und Rollenverteilung bei der wirtschaftlichen Landesverteidigung aus staatlicher, wirtschaftlicher und gesellschaftlicher Perspektive. Dabei sollen die unterschiedlichen Ausprägungen in der Vorbereitungs- und Ereignisbewältigungsphase bedacht werden
- Bestimmung eines differenzierten österreichischen Handlungsspielraums auf Basis der entwickelten Verwundbarkeits- und Abhängigkeitskategorien – reichend von weitgehender Autonomie über begrenztem Gestaltungsspielraum bis hin zu definitiver Abhängigkeit – unter Einbettung des österreichischen Wirtschaftsraums in einen europäischen und globalen Zusammenhang. Dabei sollen auch bewusst-intentionale Aktivitäten berücksichtigt werden, die der österreichischen Wirtschaft potenziell schaden können
- Erstellung einer Risikolandkarte für die österreichische Wirtschaft mit Kategorisierung der Angriffsvektoren, Verwundbarkeiten und Abhängigkeiten. Dabei sollen die bestehenden risikominimierenden Maßnahmen zur Erhöhung der Resilienz ebenso dargestellt werden. Die verbleibenden Lücken sind zu identifizieren, zu priorisieren und mögliche Handlungsoptionen zu entwickeln
- Ausarbeitung eines konzeptionellen Instrumentariums zur Verbesserung der Resilienz der österreichischen Wirtschaft, wie z.B. Kompensation, Substitution oder Information. Dieses Instrumentarium ist die Voraussetzung für eine rasche

Reaktion eines Unternehmens bei disruptiven Ereignissen, sei es in der Liefer- oder Wertschöpfungskette, auf Kundenseite oder bei den Produktionsmitteln
- Beurteilung der aktuellen Reaktionsfähigkeit der österreichischen Wirtschaft auf disruptive wirtschaftliche Verwerfungen unter Bedachtnahme der Aufrechterhaltung der Versorgungssicherheit für Bevölkerung und Wirtschaft. Dabei ist die Integration in ein europäisches Gesamtkonzept vorzusehen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.15 Erhebung des Versorgungsbedarfes von Blaulicht- und anderen krisenrelevanten Organisationen

Kontakt: Bundesministerium für Arbeit und Wirtschaft, Sektion VI – Nationale Marktstrategien, Referat VI/9a – Krisenmanagement, Ing. Mag. Michael Stern (BMAW)
E-Mail: michael.stern@bmaw.gv.at

Die umfassenden Auswirkungen und Herausforderungen von Krisen sind insbesondere in Zusammenhang mit der Covid-19-Pandemie und dem Russland-Ukraine-Konflikt auch in Österreich deutlich geworden. Die damit einhergehenden massiven wirtschaftlichen Konsequenzen, von Unterbrechungen der Lieferketten über Rohstoffknappheit bis hin zu Teuerung, haben die Bedeutung von Resilienz und Krisenfestigkeit als Grundlagen einer erfolgreichen und versorgungssicheren, standortpolitischen Entwicklung hervorgehoben. Als wichtigstes Bestandteil jeder Krisenvorsorge zeigt sich aber die Erhebung des standardisierten Versorgungsbedarfes ALLER taxativ zu erfassenden krisenrelevanten Organisationen analog der Verbrauchssätze des ÖBH. Hierzu müssten an Hand von EISENSTADT und Bezirk, ST. PÖLTEN und Bezirk sowie LINZ/HÖRSCHING und Bezirk LINZ Land alle krisenrelevanten Einrichtungen/ Organisationen (neben Polizei, Rettung, Feuerwehr auch z. B. Bestattungsunternehmen, Justizanstalten u.ä.) erfasst und der tatsächliche Verbrauch (Treibstoff, Nahrung, Wasser, Strom, Kommunikationsmittel, Batterien, etc.) für Erfüllung der zu erwartenden Aufgaben erfasst werden, auch unter Berücksichtigung jahreszeitlicher Faktoren. Diese Daten wären Basis für aufzubauende Vorratshaltung, umfassende Lagerlogistik, etc. Zusätzlich müsste ein standardisiertes Meldeverfahren entwickelt werden, welches österreichweit ausgerollt werden könnte.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation und taxative Auflistung ALLER Blaulichtorganisationen und weiterer krisenrelevanter Organisationen.
- Erfassung des Versorgungsbedarfes für 14-Tage mit Erhebung der derzeitigen Reserven der krisenrelevanten Organisationen.
- Analyse, wie weit eine signifikante jahreszeitliche Schwankung innerhalb des Versorgungsbedarfes der krisenrelevanten Organisationen besteht.
- Erhebung der derzeitig vorhandenen Reserven (Festlegung Stichtag) und des konkreten Bedarfes, um damit konkrete Lagerlogistik und Beschaffung zu planen.

- Skizzierung einer zukünftigen Versorgungsstrategie bzw. Ressourcenvorhaltesystems für Blaulichtorganisationen und weiterer krisenrelevanter Organisationen im flächendeckenden Krisenfall in der Dauer von zumindest 14 Tagen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.16 Föderierter Datenraum für GSVP-Missionen

Kontakt: Bundesministerium für europäische und internationalen Angelegenheiten, Mag. Philipp Agathonos (BMEIA)
E-Mail: Philipp.agathonos@bmeia.gv.at

Schaffung eines Datenmarktplatzes (Data Space) für internationale Sicherheitsbehörden zur Steigerung der Effektivität von Missionen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU (GSVP) und Senkung der Vorbereitungszeit für Planung und Vorbereitung von solchen Missionen (einschließlich jener mit österreichischer Beteiligung).

Bei der Schaffung eines Data Space für sicherheitsrelevante Informationen existiert bisher in der EU keine klare Regelung, zu welchen Bedingungen nicht-personenbezogene Daten von öffentlichen Stellen, anderen Unternehmen oder Personen genutzt werden können und wer in welcher Weise darauf zugreifen darf. Das Forschungsvorhaben soll deshalb untersuchen in welcher Weise die neuen legistischen Vorgaben der EU, insbesondere Data Act (DA), Data Governance Act (DGA), und AI Act effektiv angewandt werden können, um die GSVP-Missionsplanung, aber auch Missionsdurchführung durch digitale Transformation grundlegend zu verbessern.

Dabei soll vor allem erhoben werden, in welcher Weise geeignete Standards und Werkzeuge (bspw. auf Basis von Gaia-X) genutzt werden können, um einen föderierten Datenraum zur Planung von GSVP-Missionen zu entwickeln. Ein solcher Datenraum soll Austausch und Nutzung von Daten zwischen Sicherheitsbehörden und privaten Unternehmen ermöglichen und damit einen wesentlichen Beitrag zur Schaffung eines global wettbewerbsfähigen Datenökosystems für Europa leisten.

Hintergrund 1: GSVP-Missionen und Operationen sind das Schlüsselinstrument der EU zur globalen Friedenserhaltung und Sicherheit. Ihr Ziel ist die Verhütung von Konflikten und Krisen sowie der Aufbau der Kapazitäten von Partnern, um damit den Schutz der Union und ihrer Bürger zu stärken.

Hintergrund 2: Gaia-X ist eine von der EU-Industrie getriebene und durch Förderprojekte einzelner EU-Mitgliedstaaten unterstützte Initiative zum Aufbau eines wettbewerbsfähigen Datenökosystems für Europa (Data Spaces). Es adressiert somit grundlegende Anforderungen der EU-Datenstrategie. Gaia-X definiert Regeln für das souveräne kommerzielle Handeln von Daten und ermöglicht so die Umsetzung neuer Geschäftsmodelle in einem freien Datenmarkt. Gaia-X legt

Spezifikationen für einen interoperablen Datenaustausch fest und realisiert Mechanismen für einen sicheren und vertrauensvollen Datenaustausch (Labels zur Definition des Sicherheitsstandards für einen Datenaustausch; Gaia-X Clearing Houses (GXCS) zur Überprüfung der Authentizität der Teilnehmer an einem Datenmarktplatz). Dafür werden entsprechende Open Source-Lösungen zur Verfügung gestellt. Damit wird Unternehmen ein rascher und günstiger Einstieg in zukünftige Datenmarktplätze ermöglicht (siehe auch Gaia-X Hub Austria https://www.gaia-x.at/).

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Daten werden für die Planung und Vorbereitung von GSVP-Missionen benötigt und wer kann diese Daten bereitstellen?
- Welche organisatorischen und rechtlichen Rahmenbedingungen sind beim Austausch bzw. der Nutzung dieser Daten zu beachten?
- Welche Standards (Kommunikationsprotokolle, Semantiken, etc.) existieren in diesem Bereich bzw. könnten hier zum Einsatz kommen?
- Wie könnten Architektur und Governance eines föderierten Datenraums zur Planung von GSVP-Missionen aussehen?
- Welche organisatorischen und technischen Schritte sind zur weiteren Umsetzung notwendig?
- Welche Vorteile ergeben sich durch einen solchen Ansatz gegenüber dem Status quo?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.17 Rechtlicher Anpassungsbedarf sowie gesamtgesellschaftliche Aspekte im Zuge der Notfallplanung zur besseren Nachverfolgbarkeit von Ausbrüchen lebensmittelbedingter sowie sonstiger übertragbarer Infektionskrankheiten durch Rückgriff auf Nutzer:innen-Daten im Anlassfall (wie z.B. Kundenkarten, Bewegungsdaten etc.)

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: florian.fellinger@gesundheitsministerium.gv.at

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)
E-Mail: karin.rainer@ages.at

In einigen EU-Staaten ist es üblich, dass Handelsketten im Falle von lebensmittelbedingten Ausbrüchen freiwillig zwecks effizienter Ursachensuche den zuständigen Behörden Kundendaten zur Verfügung stellen. Dadurch können Quellen wesentlich schneller eruiert werden als wie ggw. durch Befragung von Erkrankten. Für die Fälle sonstiger nicht pandemischer Infektionen wären Bewegungsdaten (Mobiltelefon) oder Reihendaten aus Analysen von Personen hilfreich, um mögliche Überträger rasch identifizieren zu können oder die Prävalenz in Gruppen zu eruieren.

Den Behörden fehlen auch oft relevante Informationen um bei Arznei- und Lebensmitteln, sowie Gütern des täglichen Bedarfs im Krisenfalle steuernd eingreifen zu können. Teils liegen relevante Information vor, werden aber, auch aus rechtlichen Gründen, nicht verknüpft. Teils fehlen Behörden Information zur Gänze sind aber der Wirtschaft bekannt.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

Welche rechtlichen Möglichkeiten bei welche Anlassfällen, Behörden/beauftragte Agenturen unter den ggw. rechtlichen Rahmenbedingungen haben bzw. ausschöpfen können, um:

- auf Daten von Kund:innen von Handelsketten zwecks Identifikation des Ursprungs und der Verbreitung von z.B. lebensmittelbedingten Krankheitsausbrüchen zuzugreifen
- die Meldung von Lagerbeständen und logistischen Hintergrund-Informationen zu Lebensmitteln und Gebrauchsgegenständen, einzufordern, um im Fall von Ausbrüchen oder Krisen rasch agieren zu können
- auf Patient:innen-Daten sowie Proben (z.B. Blutproben, Harn,…) zugreifen zu können, um die Verbreitung von Infektionen in der Bevölkerung rasch nachvollziehen und Maßnahmen zur Eindämmung zielgerichtet setzen zu können
- auf Daten von Produktionsbetrieben sowie Heimtierhalter:innen im Fall von Zoonosen zugreifen zu können.

Mit evaluiert werden soll, welche relevanten Daten derzeit überhaupt vorhanden sind, wo sie gespeichert sind und welche Möglichkeiten des Zugriffes es derzeit gibt. Des Weiteren sind rechtliche Gestaltungsmöglichkeiten im gegenwärtigen rechtlichen Verfassungsrahmen in Österreich und deren Optimierungspotenzial zu untersuchen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.18 Klimaschutz als zentrale Basis für die umfassende Sicherung der Infrastruktur im Gesundheitssektor und der Gesundheitsversorgung

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: Manfred.Ditto@gesundheitsministerium.gv.at

Kontakt: Gesundheit Österreich GmbH (GÖG)
E-Mail: ruperta.lichtenecker@goeg.at

Klimaschutz ist - angesichts rechtlicher Verpflichtungen und auf Grund der gravierenden Folgen der Klimakrise auf die kritische Infrastruktur und der damit einhergehenden erforderlichen Maßnahmen - prioritär und umfassend in allen Bereichen umzusetzen. Das Gesundheitswesen hat in Österreich einen Anteil von 6,7 Prozent am nationalen Fußabdruck.

Zentral sind die Reduktion und Effizienz der eingesetzten Energie und Ressourcen im Gesundheitswesen z.B. durch:

- Erhöhung der Energieeffizienz und Reduktion des Energieverbrauchs,
- dem Einsatz Erneuerbarer Energie
- der Stärkung der Kreislaufwirtschaft
- die Reduktion des Ressourcenverbrauchs und
- der Forcierung der Sicherung der Lieferketten durch nachhaltige Beschaffung von Arzneimittel und Medizinprodukten.

Die Implementierung von Maßnahmen des Klimaschutzes bedeutet auch die Sicherung der Infrastruktur, Stärkung der Unabhängigkeit und dient dem Schutz der erforderlichen Funktionsfähigkeit des Gesundheitswesens. Damit soll die Versorgung in Form von Gesundheitsdienstleistungen für die Bürger:innen langfristig und nachhaltig gesichert werden, um wiederum die Sicherheit insgesamt zu gewährleisten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

Dazu braucht es die Gestaltung von Rahmenbedingungen (z.B. Governance, Monitoring und Indikatoren, Strategische und rechtliche Rahmenbedingungen, Telemedizin etc.) und Maßnahmen in allen Handlungsfeldern (Gebäude, Energie, Transport und Mobilität, Ressourcenmanagement, Beschaffungswesen etc.). Die genannten Bereiche gilt es in ihrer spezifischen Ausgestaltung für das Gesundheitswesen zu erforschen und zu definieren und damit die Versorgungssicherheit zu stärken.

Das ist ein zentraler Beitrag zur Sicherung der kritischen Infrastruktur im Gesundheitswesen!

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.19 Psychosoziale Resilienz der Beschäftigten in kritischen Infrastrukturen

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: hristina.dietscher@gesundheitsministerium.at

Kontakt: Gesundheit Österreich GmbH (GÖG)
E-Mail: alexander.grabenhofer-eggerth@goeg.at

Kontakt: Bundesministerium für Arbeit und Wirtschaft (BMAW)
E-Mail: julia.steurer@bmaw.gv.at

Die Covid-19 Pandemie und die Maßnahmen zu ihrer Bewältigung und die allgemeine multiple Krisenlage (Teuerung, Energie, Klima, Krieg) brachten und bringen beträchtliche psychische Belastungen für die gesamte Bevölkerung mit sich, wie durch zahlreiche Studien bzw. die vom BMSGKP beauftragte „Surveillance psychische Gesundheit“ belegt werden konnte. Besonders betroffen sind

Jugendliche und junge Erwachsene, Menschen die Mehrfachbelastungen ausgesetzt sind, Frauen, Alleinstehende und Menschen, die schon vorher in (gesundheitlichen, sozialen, ökonomischen) Problemlagen waren. Im Bereich des Gesundheitspersonals sind ebenfalls negative Langzeitauswirkungen durch die pandemiebedingte erhöhte Belastung zu sehen und ein wesentlicher Grund für das Wechseln des Jobs. Internationale Studien zu bisherigen Krisen- bzw. Katastrophenereignissen zeigen, dass die psychosozialen Folgen die Phase der eigentlichen Krise bei weitem überdauern (Banks et al. 2021).

Im Zuge der Pandemie wurde der zentrale Stellenwert von Gesundheits- und Sozialsystemen bzw. von „kritischen Infrastrukturen" hinsichtlich der Gewährleistung von Versorgungssicherheit, aber auch für die Aufrechterhaltung sozialer Sicherheit und Stabilität deutlich. Als kritische Services bzw. Infrastrukturen werden jene Infrastrukturen definiert, deren Nichtweiterführung hohe gesellschaftliche Kosten mit sich bringt. Beispiele für kritische Services sind Gesundheits- und Pflegeeinrichtungen, Blaulichtorganisationen, Lebensmittelhändler, Apotheken, IT-Services und Energieversorger (BMSGKP (Hg.) (2022): COVID-19-Pandemie. Bestandsaufnahme und Handlungsrahmen. Version 2.0).

Mitarbeiter:innen der kritischen Infrastruktur – insbesondere des Gesundheitswesens – gehören zu besonders belasteten Bevölkerungsgruppen. Die Covid-19 Situation bedeutete für diese Mitarbeiter:innen erhöhten Stress und stellt ein Risiko für ihre psychische Gesundheit dar. Ein hoher Anteil des Gesundheitspersonals zeigte beispielsweise Symptome von posttraumatischen Stress-Symptomen, Depression, Angst oder Schlafstörungen (Barbara, Juen (Universität Innsbruck, Österr. Rotes Kreuz); Monika, Stickler (Österr. Rotes Kreuz) ((Hg.): Empfehlungen für die psychosoziale Unterstützung des Krankenhauspersonals in COVID-19). In der kritischen Infrastruktur beschäftigte Personen sind im Rahmen der COVID-19-Pandemie vielfach gefordert gewesen, körperlich und psychisch, akut und über einen langen Zeitraum. Personen wurden an und über Belastungsgrenzen gebracht, um ein Funktionieren und Aufrechterhalten des Systems zu allen Zeiten zu gewährleisten und neben der COVID-19-relevanten Versorgung auch die Regelversorgung sicherzustellen, oft war der Ausstieg aus dem Job die Folge. Psychische Belastungen von Mitarbeiter:innen der kritischen Infrastruktur und damit in Zusammenhang stehende potenzielle Ausfälle können zu einer ohnehin brisanten Planbarkeit, weniger Verlässlichkeit und größerer Unsicherheit bezüglich gesellschaftlich relevanter Versorgungsaufgaben führen.

Allerdings zeigte sich insbesondere im Gesundheitsbereich auch, dass viele der Belastungsfaktoren bereits vor der Pandemie spür- und messbar waren und durch die Pandemie nur noch weiter verstärkt wurden. Es sind daher sowohl Maßnahmen auf individueller Ebene als auch auf organisatorischer Ebene notwendig, um den Beschäftigten in kritischen Infrastrukturen hier entsprechende Unterstützung und Entlastung zu bieten bzw. ihre psychosoziale Resilienz zu stärken (Barbara, Juen; Alexander, Kreh et. al (2021): Effekte der Covid-19 Pandemie auf das Gesundheitspersonal: organisatorische Risiko- und Schutzfaktoren. In: Trauma – Zeitschrift für Psychotraumatologie und ihre Anwendungen. 19 Jg. (2021) Heft 3).

Resilienz ist die Kraft, sich zu erholen. Es ist eine Fähigkeit, ein relativ stabiles und gesundes Maß an psychischer und körperlicher Kompetenz aufrechtzuerhalten, auch wenn man kritischen Ereignissen bzw. extremen Stressoren ausgesetzt ist (Bonanno, G. A. (2004). Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive After Extremely Aversive Events? American Psychologist, 59(1), 20–28). Resilienz ist allerdings keine rein individuelle Personeneigenschaft, sondern bestimmt sich immer aus Person- UND Umweltfaktoren (Juen, Barbara, Siller, Heidi & Nindl, Sandra (2013). Resilienz als sozialer Prozess, Gruppenpsychotherapie und Gruppendynamik 49: 238 – 251 (2013)). Insofern ist anzunehmen, dass erfolgreiche Maßnahmen zur Minderung der Belastungsfolgen und zur Steigerung der Resilienz breit (an multiplen Faktoren) ansetzen und über die individuelle Ebene (z.B. „psychologische Sprechstunde“) hinausgehen müssen. Organisationale Resilienz muss bei Rahmenbedingungen wie Ausbildung, Bezahlung, Arbeitsbedingungen und adäquater Kommunikation ansetzen.

Während die Effekte und mögliche Schutzfaktoren für das Gesundheitspersonal grundsätzlich relativ gut untersucht sind, gibt es wenig leicht verfügbares Wissen über effektive Maßnahmen zur Resilienzförderung. Im Rahmen dieses Projekts soll erhoben werden, welche nationalen und internationalen Studienergebnisse und Beispiele guter Praxis zur Resilienzförderung, Belastungsreduktion und letztendlich Attraktivierung der Jobs in der kritischen Infrastruktur zu finden sind und ob sie sich für die Übertragbarkeit auf österreichische Verhältnisse eignen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Eingrenzung der einzubeziehenden Berufsgruppen bzw. Bereiche der kritischen Infrastruktur (wer sind die vulnerabelsten Gruppen? Welche Art von „Bedrohung“ haben die Mitarbeiter:innen in den unterschiedlichen Bereichen der kritischen Infrastruktur?)
- Gezielte und differenzierte Erhebung von nationalen und internationalen Studien zu Belastungen in jeweiligen Berufsgruppen/Bereichen
- Differenzierte Erhebung von Studien und good practice Beispielen zu geeigneten Maßnahmen der Resilienzförderung und Belastungsreduktion
- Basierend auf den Ergebnissen Aufzeigen von Möglichkeiten zur Verbesserung der psychosozialen Resilienz der Beschäftigten in kritischen Infrastrukturen
- Ableitung von konkreten und anwendungsorientierten Umsetzungsempfehlungen für die Bereiche der kritischen Infrastruktur unter Einbeziehung der betroffenen Bereiche
- Priorisierung erster konkreter Implementierungsschritte.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.20 Early Warning Tool zur Bewertung internationaler Versorgungsunterbrechungen der österreichischen Agrargüter- und Lebensmittelproduktion

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abteilung II/8 (BML)
E-Mail: abt-28@bml.gv.at

Österreich ist als kleine offene Volkswirtschaft internationalen Entwicklungen besonders stark ausgesetzt. Große Länder wie die USA können im eigenen Wirkungsbereich weitreichende Maßnahmen zur Stabilisierung von Lieferketten setzen. Österreichs Handlungsspielraum wird maßgeblich vom Verhalten von Akteuren im Ausland beeinflusst. Um Instrumente für einen wirkungsvollen Einsatz von nationalen und EU-weiten Lenkungsmaßnahmen zu entwickeln, ist es nötig, die Wirkungskanäle von internationalen Schocks zu kennen, diese zu verstehen und ihre Auswirkungen auf die Wertschöpfungskette Agrargüter und Lebensmittel quantitativ simulieren zu können. Dazu gibt es bereits mehrere Lösungsansätze, die aber bisher noch nicht für diesen Zweck eingesetzt wurden. Die Zielstellung ist dabei nicht die operative Entscheidungsunterstützung, sondern die strategische.

Mit dem Projekt ROBVEK (Robuste Versorgungsketten) wurde unter anderem ein Dashboard zur Analyse und Visualisierung internationaler Handelsdaten entwickelt. Es zeigt die systemische Abhängigkeit der österreichischen Lebensmittelproduktion von wichtigen Rohstoffen und Vorleistungen aus dem Ausland. Kennzahlen beschreiben die Änderung der Abhängigkeit von Ländern mit unterschiedlichem Risikoprofil.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Weiterentwicklung des ROBVEK-Dashboards, um den Informationsgehalt für Entscheidungsträger:innen in mehreren Dimensionen zu erhöhen
- Erweiterung des systemischen Risikomonitorings auf der Grundlage der entwickelten Methode auf weitere Rohstoffe und Vorleistungen für Agrar- und Lebensmittelproduktion
- Review von Methoden, um den Nachteil in der vorliegenden Implementierung, die mangelnden Aktualität, zu beseitigen und gegebenenfalls die Implementierung geeigneter Lösungsansätze
- Analyse der Preistransmission für wichtige Agrargüter, Lebensmittel und Vorleistungsprodukte zur Beurteilung der Effekte von internationalen Preisschocks (Ausmaß, Geschwindigkeit und Zeitdauer) auf österreichische Lebensmittelpreise
- Erweiterung der bestehenden stark vereinfachten Input-Output-Struktur des bestehenden Modells der österreichischen Volkswirtschaft mit einem differenzierten Agrarsektor und der Struktur der Lebensmittelproduktion.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.21 Wissensmanagementsysteme zur effizienten Entwicklung von Strategien im Sicherheitsbereich

Kontakt: Bundesministerium für europäische und internationale Angelegenheiten, Abteilung VI.7 – IKT, Abteilungsleiter Mag. Kristian Jurić (BMEIA)
E-Mail: kristian.juric@bmeia.gv.at

In der heutigen datengesteuerten Welt stehen Behörden vor der Herausforderung, große Mengen an strukturierten und unstrukturierten Daten zu verwalten und daraus wertvolle Erkenntnisse zu gewinnen. Herkömmliche Informationsmanagementsysteme haben oft Schwierigkeiten, relevante Informationen effizient zu verarbeiten und abzurufen, was zu Ineffizienzen und verpassten Analysegelegenheiten führt. Die neuesten Fortschritte im Bereich des maschinellen Lernens und der künstlichen Intelligenz bieten viele Ansätze, die die Funktionalität dieser Systeme drastisch verbessern könnten. Im Rahmen eines F&E-Vorhabens soll die Integration modernster maschineller Lerntechniken, semantischer Suche und großer Sprachmodelle (Large Language Models oder LLMs), in Informationsmanagementsysteme untersucht werden. Ziel ist es, Anforderungen zu erheben und ein geeignetes Systemdesign zu entwerfen, das die Wissensentdeckung und die Genauigkeit der Informationsbeschaffung verbessert und effektivere Entscheidungsprozesse ermöglicht. Der konkrete Forschungsbedarf gestaltet sich wie folgt:

- Lücken-Analyse (Gap-Analysis) in den bestehenden behördlichen Informationsmanagementsystemen und Ermittlung ihrer Grenzen bei der Entdeckung und Abfrage von Wissen
- Wie lassen sich semantische Suche und große Sprachmodelle am besten in bestehende Wissensmanagementsysteme integrieren?
- Ermittlung potenzieller Herausforderungen und Erarbeitung von Lösungsvorschlägen für die Skalierung der Integration zur Verarbeitung großer und heterogene multimodale Datensätze
- Wie kann die Leistung eines Systems im Hinblick auf die Genauigkeit der Informationsbeschaffung, die Effizienz und die Zufriedenheit der Nutzer bewertet werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.22 Explorationsstudie zu einem kompakten und einfach einsetzbarem Spürroboter für Einsatzkräfte

Kontakt: Österreichischer Bundesfeuerwehrverband (ÖBFV)
E-Mail: gerald.czech@feuerwehr.or.at

Das Vorhandensein unbekannter Gase oder anderer gefährlicher Stoffe sowie die unbekannte Konzentration solcher Stoffe (Vergiftung, Explosionsgefahr) stellt eine erhebliche Gefahr für Einsatzkräfte dar. Ein Beispiel ist der Gasaustritt mit anschließender Explosion in Ansfelden. Zwar gibt es mittlerweile gute kompakte

Sensormodule für eine Reihe von Gefahrstoffen, die das Vorhandensein und die Konzentration gut erfassen können, allerdings werde diese üblicherweise am Körper getragen. Damit ist die Einsatzkraft unter Umständen zum Zeitpunkt der Detektion bereits dem Gefahrstoff ausgesetzt oder befindet sich bereits in einer explosionsgefährdeten Umgebung.

Um einen verbesserten Schutz der Einsatzkräfte zu gewährleisten und eine verbesserte Situationseinschätzung ohne direktes Betreten des Gefahrenbereichs zu ermöglichen, wäre der Einsatz einfacher, kompakter und kostengünstiger Spürroboter wünschenswert. Diese wurde bereits im KIRAS-Projekt ROBO-MOLE grundsätzlich demonstriert, woraus folgende Eigenschaften an die Trägerplattform abgeleitet wurden:

- Kompaktheit, um einfach eingesetzt zu werden
- Kosteneffizienz, um einen Einsatz in der Breite zu erlauben und auch in schwierigen Situationen im Fall der Fälle als Verlust abgeschrieben werden zu können
- ausreichend Mobilität in urbanen Umgebungen und Gebäuden
- Robustheit in Bezug auf Funkverbindung und Steuerung über eine Entfernung von 100m.

Bei dem Spürroboter sollte es sich um eine mobile Trägerplattform handeln, die gängige Sensorsysteme für Gefahrstoffe tragen kann und per Funk sowohl gesteuert werden kann, als auch Messwerte übertragen kann.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Verfeinerung der Anwendungsfälle und Anforderungen in Zusammenarbeit mit Einsatzorganisationen
- Marktübersicht geeigneter kommerzieller Trägersystem auch aus benachbarten Domänen oder dem Consumer Bereich
- Anwendbarkeit und Grenzen des DIN Standard SPEC 91477 evaluieren
- Erarbeitung einer robusten Systemarchitektur unter dem Gesichtspunkt der Modularität
- Erstellung eines Prototypensystems
- Erstellung eines Evaluierungskonzeptes und Kriterien (KPIs)
- Durchführung einer realitätsnahen praktischen Evaluierung
- Ableitung von Folgerungen für die Erweiterung von Taktik und Ausbildung.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.23 Chancen und Möglichkeiten für den Aufbau einer „Community of Users“ für die zivile Sicherheitsforschung in Österreich

Kontakt: Österreichischer Bundesfeuerwehrverband (ÖBFV)
E-Mail: gerald.czech@feuerwehr.or.at

Krisen und Katastrophen sind Querschnittsprobleme, die einer gesamtgesellschaftlichen Bearbeitung bedürfen. Entsprechend gelten die Vernetzung und Kooperation von Wissenschaft, Praxis und Wirtschaft auch als Garant für praxisrelevante Sicherheitsforschung und Entwicklung bedarfsgerechter Lösungen. Praxisakteure, wie z.B. Behörden, Einsatzorganisationen, Non-Profit-Organisationen oder Betreiber kritischer Infrastrukturen, übernehmen zunehmend eine Schlüsselrolle in transdisziplinären Projekten und Initiativen, die weit über ihre „Bedarfsträgerschaft“ hinausreicht. Als Bedarfsträger und Zielgruppe für entwickelte Lösungen („Endanwender“) sind sie nicht nur konstitutiv für die Forschungsprobleme, sondern auch Träger projektrelevanter Expertise und Erfahrung. Zudem wirken sie in partizipativen Ansätzen zunehmend an Forschungsdesigns und -methoden (z.B. User Experience Design), vor allem aber an Bedarfserhebungen und Analysen mit und übernehmen damit eine aktive Forscherrolle. Überdies stellen sie benötigte Forschungsinfrastruktur bereit (z.B. Demonstrationen und Prototypentests im Rahmen von Übungen oder am Beispiel der Forschungs- & Entwicklungs-Stützpunkte im Feuerwehrwesen sogar unter Realbedingungen) und fungieren als wertvolle Multiplikatoren in der Dissemination von Forschungsergebnissen in die Praxis. Das Augenmerk liegt nicht nur auf der wissenschaftlichen Problemlösung, sondern auf einer in das Gesamtsystem der Gefahrenabwehr integrierten Anwendbarkeit der Lösung.

In der Realität vieler Forschungsprojekte und -initiativen laufen allerdings vielfältige Herausforderungen diesem Potenzial transdisziplinären Arbeitens zuwider. Zunächst sind Bedarfsträger häufig nicht oder nur wenig mit den Strukturen und Prozessen transdisziplinärer Projektarbeit vertraut. Die Beteiligung an entsprechenden Projekten und Initiativen ist dementsprechend häufig „unbekanntes Terrain“ oder erfolgt oftmals zu spät. Potenziellen Interessenten ohne bisherige Anbindung fehlen die Möglichkeiten, Bedarfe bzw. innovative Projektideen einzubringen und die eigentliche Projektarbeit ist häufig mit unverhältnismäßig hohem Aufwand, z.B. bürokratischer Natur (Antragsstellung, Abrechnung, Berichtlegung etc.) verbunden oder wird durch Vorbehalte erschwert. Überdies folgen Praxis, Wissenschaft und Wirtschaft unterschiedlichen Gesetzmäßigkeiten. Daraus resultieren projektintern nicht nur unterschiedliche Foki und Schwerpunktsetzungen, sondern auch divergierende oder gar konfligierende Interessen, die sich auf den Verlauf und die Ergebnisse von Forschungsprojekten auswirken können. Überdies können Verständigungsprobleme (z.B. verschiedene Herangehensweisen, Terminologien) oder informelle Hierarchien (z.B. Anerkennungsprobleme), dem Projekterfolg entgegenstehen.

Die Ausbildung einer „Community of Users“ für die zivile Sicherheitsforschung in Österreich könnte hier in vielfältiger Weise Abhilfe schaffen und als Drehscheibe für Unterstützungsangebote, langfristig angelegter Erfahrungs- und Informationsaustausch und Verständigung, Vermittlung von Forschungspartnern, sowie Projektergebnissen, u.a. dienen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Definition der Eckpunkte und langfristigen Perspektive einer „Community of Users“ für die zivile Sicherheitsforschung in Österreich
- Festlegung des potenziellen Teilnehmerkreises („Bedarfsträgerlandkarte“)
- Bestimmung von Anreizstrukturen zur Förderung der aktiven Mitwirkung durch Bedarfsträger in einer Community of Users und transdisziplinären Forschungsprojekten
- Entwicklung von Strategien und Maßnahmen zum aktiven Community Building
- Bedarfserhebung relevanter Unterstützungsangebote und Konzepterstellung für Ziele und Leistungen der „Community of Users“ (z.B. Peer-Support, Informationsdienst, Vernetzungsveranstaltungen, etc.)
- Aufbau einer „Community of Users“
- Öffentlichkeitsarbeit und Dissemination der Netzwerkinitiative und Mitgliederwerbung, sowie Verbindungsaufbau zu Partnerinitiativen im europäischen Kontext und zur Community for European Research and Innovation for Security (CERIS)
- Erstellung eines Konzepts für die Verwaltung und Administration der Community
- Continuity Management: Konzepterstellung für die langfristige Netzwerkadministration durch Trägerorganisationen, bevorzugter Anschluss an bestehende Strukturen und Netzwerkinitiativen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.24 Informelle Hilfe in Krisenzeiten

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF)
E-Mail: Mag. Dipl.-Ing. Bernhard Futter, Bernhard.Futter@bmbwf.gv.at

Informelle Hilfe funktioniert in verschiedenen Krisen schnell, pragmatisch und lokal sehr effizient – das zeigen internationale Beispiele. Bisher noch nicht ausgeschöpftes Forschungspotenzial zeigt sich besonders an der Schnittstelle unterschiedlicher Politikbereiche. In bestimmten Politikbereichen, etwa im Sozial- und Gesundheitsbereich, stellt die IH schon jetzt eine nicht wegzudenkende Säule der Leistungserbring dar. Dort zeigt sich, dass eine IH besonders für die vulnerable Population wichtig ist, da sich diese in der Ohnmacht über das krisenhafte Ereignis durch IH ermächtigt fühlen kann. Hingegen wurden bisher kaum Analysen mit Bezug zur intersektoralen Krisenbewältigung durchgeführt, etwa für Pandemien, klimatische Ereignisse oder sozioökonomische Krisen. Es erscheint daher dringlich, die Funktionsweise der IH besser zu verstehen, um sie mit der formellen Hilfe von Expertinnen und Experten bzw. professionellen (Einsatz-)kräften effizient in Verbindung setzen zu können.

Ein besonderer Fokus soll auf der Einbeziehung jener liegen, die selbst Informelle Hilfe geleistet haben, oder von Informeller Hilfe profitiert haben. Das Forschungsthema soll daher im Sinne von Citizen Science insbesondere Menschen in

den Mittelpunkt rücken, die in solchen informellen Hilfsstrukturen und Netzwerken gut verankert sind und diese Strukturen und Wirkungsweisen auf wissenschaftlicher Basis, mit wissenschaftlicher Unterstützung untersuchen wollen. Das Thema soll von den Betroffenen bzw. Beteiligten selbst (mit)beforscht werden, sie sollen Akteur/innen der Forschung sein.

Ziel des Forschungsvorhabens soll es sein, internationale Evidenz zum Thema informelle Hilfe zusammenzutragen und in angewandter Weise für den Bedarf in Österreich auszuwerten und verfügbar zu machen. Weiters soll die Funktionsweise (Akteurinnen und Akteure, Leistungen, Dimensionen, Organisation, Kommunikation, Chancen und Limitationen) von IH für österreichische Case-Studies im Normal- und Krisenfall umfassend dargestellt werden. Als Endprodukt des Forschungsvorhabens soll ein Leitfaden zur IH für relevante Stakeholder zur Verfügung gestellt werden. Im Vordergrund sollte dabei eine effektive Synergie der IH mit der professionellen Krisenbewältigung sein.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie funktioniert(e) in kommunalen Netzwerken Informelle Hilfe der Bevölkerung und wie kann diese Ressource zur Krisenbewältigung mit formalen Hilfsangeboten verknüpft werden?
- Wie erlebt die Bevölkerung IH im Normalfall und wie erlebte sie diese in bisherigen Krisen?
- Theoretische und definitorische Auseinandersetzung mit dem Begriff der IH
- Akteure und Leistungsspektrum der IH
- Evidenz zur internen Organisation und Kommunikation von IH
- Dimensionen und Determinanten, die zum Gelingen von IH beitragen
- Evidenz zu erfolgreichem Schnittstellenmanagement zur professionellen Hilfe, zu unterschiedlichen Politikbereichen und Medien
- Internationale Best-Practice Beispiele
- Wie kann IH bei zukünftigen Krisen synergetisch effizient mit professioneller Hilfe und unterschiedlichen Politikbereichen zur Krisenbewältigung beitragen?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.25 Geistige Landesverteidigung – Vorwissen und Interessen von Schülerinnen und Schülern der Sekundarstufen I und II an sicherheitspolitischen Fragestellungen

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF)
E-Mail: AL Mag. Manfred Wirtitsch, manfred.wirtitsch@bmbwf.gv.at

Geistige Landesverteidigung (GLV) ist neben der militärischen, der wirtschaftlichen und der zivilen Landesverteidigung Teil der Umfassenden Landesverteidigung (Bundesverfassung Art. 9a). Damit unterstützt GLV im Rahmen der Politischen Bildung die Vermittlung demokratischer Werthaltungen und eines umfassenden Bewusstseins für die Sicherstellung von staatlicher Souveränität und Neutralität, der demokratischen Freiheiten und der in der Bundesverfassung verankerten Bürger-

und Menschenrechte. GLV leistet weiters einen wichtigen Beitrag zum Verständnis des Konzeptes der umfassenden nationalen Sicherheitspolitik im europäischen und globalen Kontext.

Die nach dem Ende des Balkankrieges der 1990er Jahre folgenden Jahre ohne militärische Konflikte in der näheren Nachbarschaft Österreichs, des Beitritts aller direkt angrenzenden Nachbarstaaten an die NATO und die Integration Österreichs in die Europäische Union haben sicherheitspolitische Themen in der Gesellschaft und in der Schule in den Hintergrund treten lassen.

Mit dem militärischen Konflikt in der Ukraine und dem Beginn des russischen Angriffskrieges vom 24. Februar 2022 ergibt sich deutlich eine Notwendigkeit, sich mit sicherheitspolitischen Themen wieder intensiver in der Schule auseinanderzusetzen.

Schon seit 2020 gibt es Bestrebungen, im Rahmen Politischer Bildung Geistige Landesverteidigung stärker zu platzieren. Insbesondere auf Ebene der Bildungsdirektion sind Kooperationen mit den Militärkommanden prädestiniert für eine Kooperation und Verankerung im Schulwesen. Als formale Voraussetzung für eine inhaltliche Auseinandersetzung sind der Grundsatzerlass zum Unterrichtsprinzip Politische Bildung 2015 sowie die Verankerung des verpflichtenden Anwendungsbereiches „umfassende Landesverteidigung; Bundesheer“ im Kontext der Wiedererlangung der Souveränität Österreichs 1955, der freiwilligen Neutralität und der Verpflichtung, diese zu verteidigen im Lehrplan „Geschichte und Politische Bildung“ der Sekundarstufe I, 4. Klasse, zu sehen.

Folgender Forschungsbedarf ergibt sich daher für die Sekundarstufen I und II:

- Entwicklung eines altersadäquaten Verständnisses von Sicherheitspolitik, Souveränität, Neutralität, Freiheit und Sicherung einer liberalen, demokratischen Gesellschaftsordnung und ihrer politischen Institutionen
- Erhebung der Wissensgrundlagen und Wissensquellen von Jugendlichen zu sicherheitspolitischen Fragestellungen
- Identifizierung der maßgeblichsten Faktoren, die eine Auseinandersetzung von Schüler/innen mit sicherheitspolitischen Themen begünstigen bzw. behindern;
- Ausarbeitung der Frage, wie bewusstseinsbildende Maßnahmen gestaltet werden können bzw. wie am Thema Haltung und Einstellung im Unterricht gearbeitet werden kann?
- Entwicklung von Lehrerfortbildungsformaten, die ein Zusammenspiel von verschiedensten Akteuren sicherheitspolitischer Fragestellungen und Aufgabenbereiche (geistige, wirtschaftliche, zivile und militärische Landesverteidigung) begünstigen und die Vermittlung eines umfassenden Bildes unter Einbeziehung aller Akteure (zB PHs, Universitäten, Informationsoffiziere, zivile Verwaltungsbehörden, Wirtschaftsunternehmen, usw.) ermöglicht.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.26 Krisen- und Katastrophenforschung – Aktuelle Entwicklungen sowie Aus-, Fort- und Weiterbildung in Österreich

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung
E-Mail: Kim Eichhorn, MSc, Kim.Eichhorn@bmbwf.gv.at

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: Kim Eichhorn, MSc, Kim.Eichhorn@bmbwf.gv.at

Die Bedeutung des gesamtstaatlichen Krisenmanagements sowie dem Zivil- und Katastrophenschutz wächst in einer immer vernetzteren Welt zunehmend. Wissenschaft und Forschung spielen eine zentrale Rolle im nationalen und internationalen Krisen- und Katastrophenmanagement. Auch in Österreich finden sich daher Bemühungen, die Katastrophenforschung voranzutreiben. Vernetzung und Kooperation von Wissenschaft, Praxis und Wirtschaft über organisatorische und disziplinäre Grenzen hinweg gelten dabei als Prämissen effektiver Krisen- und Katastrophenforschung. Wie in anderen Querschnittsbereichen ist das Forschungsfeld durch Fragmentierung geprägt. Ebenso gibt es Entwicklungspotenzial bei institutionellen Rahmenbedingungen, wie etwa universitärer Verankerung. Aktuelle Auseinandersetzungen zur mittel- bis langfristigen Zielorientierung im Forschungsfeld untermauern diese Herausforderung. Entsprechende Steuerungsinstrumente erfordern ein klares Verständnis der Topografie der Forschungslandschaft, um den Wissensstand, Trends, Herausforderungen und Kapazitäten zu identifizieren.

Traditionell erfolgt die Aus- und Weiterbildung im Zivil- und Katastrophenschutz organisationsbezogen an den Ausbildungsstätten der Einsatzorganisationen bzw. der Länder. Die Natur- und Katastrophenereignisse der 1990er und 2000er Jahre haben in Österreich den Anstoß für bundesweite Ausbildungsangebote im Staatlichen Krisen- und Katastrophenschutz-management bzw. auf universitärer Ebene gegeben. Globale Ereignisse, wie die COVID-19-Pandemie, die Blackout-Problematik, der russische Krieg gegen die Ukraine oder die Klimaerwärmung, zeigen die Notwendigkeit einer gesamtstaatlichen Betrachtung auf.

Forschungsbedarf ist eine umfassende Statuserhebung für Österreich:

- Welche Themenschwerpunkte wurden und werden in der österreichischen Katastrophenforschung bearbeitet? Wo bestehen Forschungslücken?
- Wie gestaltet sich das Bildungsangebot im Krisen- und Katastrophenmanagement (Studien, Kurse, Lehrgänge, einzelne Lehrveranstaltungen) und wo gibt es noch Bedarf?
- Welche methodischen und konzeptionellen Zugänge dominieren in Österreich? Lassen sich Paradigmen und Paradigmenwechsel identifizieren? Welche Themenkonjunkturen lassen sich identifizieren? Analyse z.B. durch Scoping Reviews, Systematic Reviews.
- Welche Akteure (Individuen, Organisationen) sind in die Entwicklung des Forschungsfeldes involviert? Wie sind die Akteure untereinander vernetzt bzw. wie gestalten sich die Kooperationszusammenhänge? Analyse z.B. durch Netzwerkanalysen, bibliometrische Analysen, Feldanalysen.

- Welche Rolle nimmt Österreich im Europäischen Umfeld ein?
- Wie gestalten sich die Schnittstellen zwischen Wissenschaft, Praxis, Politik, Wirtschaft und Bevölkerung?
- Wie sind die institutionellen Rahmenbedingungen in Österreich gestaltet?
- Welche Stärken, Schwächen, Chancen und Risiken lassen sich Bezug nehmend auf die Weiterentwicklung des aus verschiedenen Perspektiven identifizieren?
- Welche Implikationen ergeben sich für die Steuerbarkeit des Forschungsfeldes?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.27 Implementierung eines automatischen Detektierungs- und Warnsystems zum Sedimentmanagement von Schlüsselbauwerken der alpinen Schutzinfrastruktur

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abt. III/4 – Wildbach- und Lawinenverbauung und Schutzwaldpolitik, DI Andreas Pichler (BML)
E-Mail: andreas.pichler@bml.gv.at

Infolge der jahrelangen Beobachtung über den fortschreitenden Feststoffabtrag in alpinen Einzugsgebieten und dessen Implikation für die vorhandene Schutzinfrastruktur (im wesentlichen Geschieberückhaltebecken und –räume) aufgrund des Klimawandels, ist eine zunehmende Beaufschlagung dieser Bauwerke durch abgelagertes Geschiebe und Feststoffeinträge (auch Wildholz) zu verzeichnen. Dies bringt die Funktionalität dieser Schutzinfrastruktur zunehmend an ihre Grenzen, was natürlich auch Auswirkungen auf das allgemeine Schutzniveau gegenüber alpinen Naturgefahren in Österreich hat. Im Zuge von Katastrophenereignissen ist dabei immer mehr die rasche Feststellung des Füllungsgrades – und damit einhergehend der Funktionsfähigkeit – der Schutzinfrastruktur notwendig, um einerseits eine frühzeitige Warnung und ev. Evakuierung von betroffenen Gebäuden/Personen einleiten zu können und andererseits effektive Gegenmaßnahmen (z.B. akute Räumung von Retentionsbecken-/räumen) vornehmen zu können.

Derzeit basiert dies in den überwiegenden Fällen auf visuelle Einschätzung durch Experten, wobei die meisten Bauwerke dieser Schutzinfrastruktur – wir sprechen über mind. 50.000 in Österreich – in steilen, meist entlegenen und oft schwer zugänglichen Gebieten liegen. Sehr oft kann dies auch nur per Helikopterflug sinnvoll festgestellt werden.

Das Ziel dieses Vorhabens wäre es, bundesweit, auf einheitlichen Standards basierend, ein automatisches Detektions- und Warnsystem im Umfeld solcher Schutzinfrastruktur aufzubauen. Die Warninformation – sobald ein gewisser Messwert überschritten wird – würde an die zuständigen Dienststellen der Wildbach- und Lawinenverbauung, der Landeswarnzentralen, Feuerwehreinsatzstäben und Gemeinden gehen, um dort umgehend Notfallmaßnahmen einleiten zu können.

Folgender Forschungs- und Entwicklungsbedarf ergibt sich in diesem Zusammenhang:

- Evaluierung der Möglichkeiten einer bundesweit einheitlichen und standardisierten Detektion des Füllungsgrades von Geschieberückhaltebecken und –räumen
- Festlegung von Toleranzgrenzen und Schwellwerten zur Auslösung von Warnungen – abhängig vom jeweiligen Bautyp
- Aufbau eines Übertragungsnetzes für Warnmeldungen – unabhängig von der aktuellen Wetterausprägung
- Möglichkeiten einer on-line Analyse und Dokumentation einer möglichen Beeinträchtigung der Funktionalität der Schutzinfrastruktur.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.28 Schutz kritischer Infrastruktur allgemein

Hier können weiterhin alle F&E-Dienstleistungen eingereicht werden, welche das Thema Schutz kritischer Infrastruktur treffen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.3 K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für kooperative F&E-Projekte

3.3.1 Die zukünftige Entwicklung kryptographischer Verfahren

Kontakt: Bundeskanzleramt (BKA)
E-Mail: isk@bka.gv.at

Die Digitalisierung und Globalisierung benötigen eine sichere Telekommunikation und diese wiederum erfordert eine sichere Kryptographie. Insbesondere sind Staaten auf den Austausch von klassifizierten Informationen zur Aufrechterhaltung der staatlichen Handlungsfähigkeit, der öffentlichen Ordnung und der internationalen Beziehungen angewiesen Darüber hinaus hat die Verwaltung eine Verpflichtung, alle ihre wichtigen und sensiblen Daten durch entsprechende Maßnahmen der Cybersicherheit zu schützen.

Die aktuelle Kryptographie baut auf der Vermutung auf, dass es mathematische Probleme gibt, die für einen Angreifer sehr schwer zu lösen sind. Diese Vermutung ist durch die Nutzung von Quantencomputer nicht mehr aufrecht zu erhalten. Somit müssen alternative Methoden gefunden werden, bevor solche Computer in der Lage sind, die mathematischen Probleme schneller zu lösen, als es die Vertraulichkeit der Information verlangt. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) und der niederländische Allgemeine Nachrichten- und Sicherheitsdienst (AIVD) gehen davon aus, dass die herkömmlichen Schlüssel klassifizierter Informationen ab 2030 nicht mehr als sicher bewertet werden können.

Besondere Schwachpunkte in der Kryptographie sind die Erzeugung und die Verteilung von Schlüsseln. Daher versucht man schon seit geraumer Zeit physikalische Methoden zu finden, die ohne die angesprochene (nicht beweisbare) Vermutung auskommen. Vier Lösungsansätze für die Erzeugung und Verteilung von Schlüsseln auf Basis physikalischer Methoden sind heute bekannt und anerkannt:

1) Verfahren mit Hilfe von verschränkten Teilchen, auch Quantum-Key-Distribution (QKD) genannt

2) QKD mit dem BB84-Protokoll durch Übertragung von polarisierten Photonen

3) Erzeugung der Schlüssel durch einen Hardwaregenerator und physische Verteilung durch hochsichere Memory Sticks (z.B: mit eigener PIN-Tastatur, integrierter AES-256 Hardwareverschlüsselung und FIPS 140-1 Level 3 Zertifizierung)

4) Verfahren, die auf der Reziprozität der Funkübertragung und Messung von Funkkanaleigenschaften basieren.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Umfangreicher Vergleich der oben genannten Verfahren aus der Sicht der Sicherheit (vor allem der Angriffsszenarien und Abwehr Dritter), Funktionalität, Marktreife und Kosten
- Technologieneutrale Analyse der Vor- und Nachteile bzw. generelle Eignung der Methoden in Bezug auf verschieden Anwendungsszenarien unter Berücksichtigung von Distanz und Übertragungsrate, wie zu Beispiel ein Behördennetzwerk, hoch-klassifizierte Netze, Cybersicherheit, Schlüsselaustausch durch Satelliten (Minimierung der Abhängigkeit terrestrischer Infrastruktur; Black-out-Szenarien; terroristische Angriffe), Schlüsseltypen, etc.
- In Hinblick auf die Bedrohungsszenarien durch Quantencomputer im Geheimschutz, eine Analyse, welche Methoden in der Praxis am schnellsten vollständig entwickelt und eingesetzt werden können, um einen lückenloses Schutz zu garantieren (theoretische Sicherheit vs. praktischer Fehlerquellen)
- Praktische Umsetzung und Tests der oben genannten Verfahren einerseits für kurze (z.B. im Umfeld eines Behördennetzwerkes) und andererseits für größere Entfernungen
- Identifizierung von weiterem Forschungs- und Entwicklungsbedarf und Potentialen zum derzeitigen Stand der Technik unter Rücksichtnahme von europäischen Entwicklungen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.2 Förderung des Wissensaustauschs in Strafverfolgungsbehörden durch NLP- und LLM-basierte Chatbots

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Strafverfolgungsbehörden nutzen interne Wissensdatenbanken, um Informationen und Wissen effizient zu speichern, zu organisieren und für den späteren Zugriff bereitzuhalten. Ein Beispiel hierfür ist der Kriminalistische Leitfaden (KLF) des BMI, der unter anderem Handlungsanweisungen für den Umgang mit Cyber-Crime-Delikten und interne Dienstanweisungen enthält. Das primäre Ziel solcher Wissensdatenbanken ist der Wissensaustausch innerhalb der Organisation und die Steigerung der Effizienz, indem Mitarbeiter Zeit einsparen können, indem sie schnell und einfach auf relevante Informationen zugreifen.

Aktuelle Entwicklungen im Bereich des Natural Language Processing (NLP) und der Large Language Models (LLM) sowie deren überzeugende Effektivität über verschiedene Anwendungsdomänen hinweg, legen den Einsatz dieser Technologien für den Wissensaustausch innerhalb von Strafverfolgungsbehörden nahe. In Zukunft könnte es möglich sein, dass Mitarbeiter mittels eines Chatbots auf das in der Organisation vorhandene Wissen zugreifen können.

Die zentrale Herausforderung besteht dabei darin, einen Ansatz zu finden, der das Potenzial moderner NLP- und LLM-Technologien ausschöpft und gleichzeitig mit den europäischen datenschutzrechtlichen und ethischen Grundsätzen vereinbar ist. Ein wesentlicher Aspekt liegt daher in der Wahrung der Datensouveränität beim Aufbau und Betrieb solcher Lösungen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können Wissensdatenbanken mit Chatbot-Funktionen erweitert werden, die auf modernen NLP- und LLM-Technologien basieren?
- Wie und in welchem Ausmaß können vortrainierte LLM-Modelle an die Anforderungen und den Wissensbestand von Strafverfolgungsbehörden angepasst werden?
- Inwiefern kann ein solcher Ansatz die Handlungssicherheit erhöhen und die Qualität von Ermittlungen verbessern?
- In welcher Weise und in welchem Ausmaß kann ein solcher Ansatz Mehrsprachigkeit unterstützen?
- Welche Strategien und Methoden können eingesetzt werden, um die Datensouveränität zu wahren?
- Wie kann ein solches Wissensmanagement-System unter Berücksichtigung europäischer Datenschutz- und ethischer Grundsätze implementiert und betrieben werden?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.3 Mobile digitale Aufnahme von Schuhspuren

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Präzision und Geschwindigkeit spielen eine entscheidende Rolle bei kriminalpolizeilichen Ermittlungen, insbesondere wenn es um die Auswertung von Schuhspuren geht. Moderne Technologien zur Beweissicherung und Identifizierung müssen diesen Anforderungen gerecht werden. Die vermehrte Nutzung biometrischer Beweise, insbesondere Schuhspuren, könnte einen bedeutenden Fortschritt für polizeiliche Ermittlungen und Gerichtsverfahren bedeuten.

Ein weiterer wichtiger Aspekt ist das Preis-Leistungs-Verhältnis der eingesetzten Werkzeuge. Es ist essenziell, dass eine verbesserte Ausrüstung nicht ausschließlich aus überbewerteten oder überteuerten Komponenten besteht. Die Grundlage für Verbesserungen sollte auf innovativen KI-basierten Algorithmen, der Entwicklung einfacher und kostengünstiger Hardware-Ergänzungen sowie der Verwendung erschwinglicher COTS-Geräte mit hoher Rechenleistung beruhen.

Die Aufnahme von Spuren wie Schuhabdrücken ist ein zeitaufwändiger Prozess, der viel kriminalistische Arbeit erfordert. Insbesondere das Anfertigen von Schuhabdrücken mittels Gießformen kann zwar immer noch vertretbar sein, aber moderne Smartphone-Aufnahmemethoden könnten hier möglicherweise eine Alternative bieten.

Insgesamt ist die Einführung moderner biometrischer Werkzeuge und Technologien in kriminalpolizeiliche Ermittlungen von großer Bedeutung, da sie die Genauigkeit und Schnelligkeit der Identifizierungsprozesse deutlich verbessern könnten. Dadurch würde nicht nur die Effizienz der Ermittlungen gesteigert, sondern auch die Sicherheit und Gerechtigkeit in Strafverfahren erhöht werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwicklung einer Anwendung für iOS zur Aufnahme von Schuhspuren
- Nutzung der Rechenleistung zur Erstellung von 3D-Modellen
- Entwickeln einer Methode zur Einspielung der Aufnahmen in das Polizeinetzwerk und entsprechender Datenbanken zur Effizienzsteigerung der Polizeiarbeit im Zusammenhang mit Schuhspurensicherung am Tatort
- Erforschen von Modellen zur Erstellung von 3D-Modellen und dadurch möglichen Qualitätsverbesserung der Arbeitsmethoden.

Ein dementsprechendes kooperatives F&E Projekt soll die Ergebnisse des KIRAS-Projekts „IT unterstützte Suche und Vergleich von Schuhspuren in einer Tatspurendatenbank und einem Schuhkatalog – impress (Projektkurztitel: Impression Evidence and Shoe Model Search – impress) berücksichtigen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.4 Entwicklung einer KI-unterstützten Werkspurensuche

Kontakt: Bundesministerium für Inneres (BMI)
E-Mail: BMI-I-A-3-SiFo@bmi.gv.at

Bei zahlreichen Einbruchsdiebstählen können Werkzeugspuren gesichert werden. Doch der Vergleich solcher Spuren von verschiedenen Tatorten gestaltet sich als äußerst zeitaufwändig. Ähnlich aussehende Spuren müssen einzeln in einem Vergleichsmikroskop mühsam gegenübergestellt und nach Gemeinsamkeiten durchsucht werden.

Ein effizientes Hilfsmittel für das Erkennen von Straftatenserien, die von derselben Täterschaft begangen wurden, könnte durch geeignete Abbildungen der Spuren (digitale Aufnahmen) und einer computergestützten Suche nach ähnlichen Werkzeugspurenmustern von anderen Tatorten in einer großen Datenbank mit Bildern von Werkzeugspuren (Datenbank) geschaffen werden. Diese Bilder würden mit zusätzlichen textuellen Metadaten versehen sein.

Dadurch können dem kriminaltechnischen Bearbeiter aus der Vielzahl von Spuren in der Datenbank die vielversprechendsten Spuren für eine weitergehende Untersuchung angeboten werden. Dies würde zu einer schnellen Zuordnung zahlreicher Straftaten aus einer Serie zu einer Täterschaft führen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung von KI-basierten Suchalgorithmen zur Klassifizierung und Zuordnung von Werkzeugspuren unterschiedlicher Tatorte
- Entwicklung unterschiedlicher bzw. angepasster Methoden für verschiedene Arten von Werkzeugspuren
- Nutzung der BMI-Ressourcen wie Datenbanken und IKT und die damit verbundene Integration der neu entwickelten Software.

Ein dementsprechendes kooperatives F&E Projekt soll die Ergebnisse des KIRAS-Projekts „IT unterstütze Suche in großen Werkzeug- und Formspurendatenbanken“ (Projektkurztitel: FORensic Marks Search - FORMS) berücksichtigen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.5 Virtual- / Mixed Reality Tool für die Bewertung von Umweltkatastrophen, zugehörige Maßnahmenplanung sowie die Post-Disaster Schadenserhebung

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Umweltkatastrophen wie Überschwemmungen oder Waldbrände nehmen auch in Österreich immer weiter zu. Für die Planung von Hilfseinsätzen sowie für die Bewertung von möglichen Auswirkungen und des Schadensausmaßes werden Tools zur Unterstützung von Entscheidungsträgern benötigt. Diese Tools und Technologien sollen Lagebilder intelligent in 3D in Echtzeit zur Abschätzung der Auswirkungen von bzw. während Naturkatastrophen visualisieren und die Konfiguration von Parametern wie z.B. Wassermenge ermöglichen. Spezifische Schritte zur Entscheidungsfindung oder Katastrophenbewältigung sollen nicht nur vor Ort, sondern auch remote planbar sein und die Lagebilder anderen Entscheidungsträgern und Einsatzkräften via MR-Technologien in Echtzeit zur Verfügung gestellt werden. Zur Abbildung und Bewertung von Schäden soll ein Labeling direkt in VR/MR durchgeführt werden können. Dadurch soll der Aufwand für die Aufnahme und Beurteilung von Schäden minimiert und der Prozess nachvollziehbar werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwickeln von Technologien zur kostengünstigen Aufnahme von großen Katastrophengebieten und Darstellung dieser in Virtual- / Mixed-Reality, möglichst in Echtzeit. Dies soll Aufnahmetechnologien aus der Luft sowie Aufnahmeverfahren mittels MR-Brillen miteinander verknüpfen
- Algorithmen-Entwicklung für die effiziente Darstellung von großen Katastrophengebieten in VR / MR
- Aufnahme und Darstellung der aktuellen Katastrophenlage in VR / MR (Sensor-Fusion, Erstellung eines Lagebildes, …)
- Möglichkeit der Remote-Betrachtung / Remote-Unterstützung für Entscheidungen, Maßnahmensetzung und Schadensbewertungen

- Entwicklung eines MR-Demonstratorsystems zur Schadensaufnahme und Labeling von Schäden vor Ort sowie remote
- Identifikation, welche Informationen in einem 3D Lagebild dargestellt werden müssen, um präzisere Entscheidungsgrundlagen vorlegen zu können.

Wichtig ist hierbei, bestehende Ergebnisse laufender oder bereits abgeschlossener KIRAS- Projekte zu berücksichtigen und vorhandene Synergien und Ergebnisse zu nutzen. Eine Zusammenarbeit mit den österreichischen Geodiensten und dem BMLV ist für den Projekterfolg notwendig. Für den weiteren Forschungsbedarf kann auf folgenden Vorerfahrungen aufgebaut werden:

- MRespond (Multi User Mixed Reality System für flexibles Training von Einsatzkräften): Im Rahmendes KIRAS geförderten Projekts MRespond wird und wurde (2021-2023) eine Mixed Reality Umgebung für Einsatzkräftetrainings geschaffen, welche einen integrierten Ansatz zur Bearbeitung von Szenarien in der Planung als auch Durchführung und Beurteilung verfolgt. Die genutzten Technologien zu Lagesetting und Beurteilungsoptionen (Übungsleiter*innen-Interface) als auch die entwickelten Tools zur Lokalisierung (indoor und outdoor) von Einsatzkräften sowie anderen Personen / Objekten für eine teils reale, teils virtuelle Interaktion unter Nutzung von Mixed Reality Brillen bietet Potential zur weiteren Verwertung in einem derartigen Folgeprojekt mit Fokus Reale Einsatzsettings
- MUSIG (Multisensor-basierte Informationsgenerierung zur Unterstützung von Krisenmanagement und Präventionsstrategien) befasst sich mit automatisierter, KI-basierter Ableitung und Fusion von Bewegungsinformationen aus geo-sozialen Medien, Mobilfunkdaten und in-situ Kamerabildern. Unter Einbezug verschiedener Szenarien werden in weiterer Folge Bewegungsinformationen durch einen mixed-methods Ansatz Behörden und Einsatzkräften in naher Echtzeit bereitgestellt, um Krisenmanagement und -prävention zu erleichtern. Zusätzlich zu der reinen Bewegungsanalyse extrahiert MUSIG auch semantische- und Stimmungsinformation.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.6 Prozessierungsframework für Lidar und bildgebende multimodale Sensordaten

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Die in den letzten Jahrzehnten gestiegenen Anforderung an Effizienzsteigerung und Ressourcen-reduzierung, sowie eine angestrebte gesteigerte Sicherheit der militärischen Einsatzkräfte sind aufgrund sich sehr dynamisch ändernder Gefahrenlagen immer schwieriger zu bewältigen.

Intelligente geo-orientierte Informationsprodukte (GEOINT) haben bei modernen Streitkräften für militärische Aufgaben deshalb an Wichtigkeit noch deutlich

gewonnen. Diese sind eine wesentliche Grundlage bzw. wichtige Unterstützung von nationalen und multinationalen C4ISR Prozessen sowie der vernetzten Operationsführung in militärischen Einsätzen. Grundsätzlich bieten unterschiedliche Trägerplattformen (Satelliten-, Flugzeug-, Hubschrauber- und Drohnen sowie terrestrische Systeme) und Sensoren (optische, IR, Radar, Lidar, etc.) einen Zugang zu umfangreichen geo-orientierten Daten.

Grundsätzlich wird auf Basis eines Gesamtkonzeptes für ein auf Lidar und bildgebende multimodale Sensordaten ausgerichtete GEOINT-Prozessierungsframework ein modularer, stufenweiser Aufbau eines Prozessierungsframeworks angestrebt.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Konzeptentwicklung für ein GEOINT-Prozessierungsframework auf Basis eines multisensoralen- (optische, IR, Radar, Lidar, etc.) und multimodalen (Satelliten-, Flugzeug-, Hubschrauber- und UAV sowie terrestrische Systeme) Gesamtansatzes
- Konkrete Umsetzung erster Module für die Bearbeitung von Flugzeug-, Hubschrauber- und UAV gestützten Multisensor-Daten. Integration von performanten Geoprozessierungs-workflows und KI/ML-basierten Analysemetroden
- Konzeption und PoC-Entwicklung eines effizienten Datenbanksystems für 2D/3D Daten inklusive einer API für schnellen und einfachen Zugriff auf definierbare region-of-interest Datenfusions-Daten (Lidar Punktwolken, Bilddaten) für ein vollständiges 2D und 3D Mapping von kritischer Infrastruktur (Gebäude indoor- und outdoor Bereiche) bzw. Truppenübungsplätzen
- Aufbereitung von Daten für die Nutzung im Flugsimulator bzw. Entwicklung von Geo-Schnittstellen für externe militärische Systeme (Lagebildsysteme, etc.).
- Entwicklung einer lizenz- und installationsfreien web-basierten Nutzerschnittstelle für die interaktive Visualisierung von 2D/3D-Mapping Daten (Punktewolken, Orthobilder, etc.) und 3D Modellen um eine gezielte, rollenorientierte Verteilung der GEOINT-Informationsprodukte zu ermöglichen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.7 Entwicklung eines Kryptosystems, welches mit österreichischem Wissen entwickelt und zukünftig im österreichischen Wirtschaftssystem produziert wird. Im Bereich der Cyber-Sicherheit ist die Verschlüsselung der Garant zur Gewährleistung des Schutzziels Vertraulichkeit

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Aktuell werden im BMLV unterschiedliche Komponenten und Systeme verwendet, wie z.B. Datenverschlüsselungsgeräte aus Deutschland oder der Schweiz. Diese Systeme halten sich an internationale Standards im Hochsicherheitsbereich und sind auch dementsprechend zugelassen, um Verschlusssachen wie z.B. EU SECRET,

übertragen zu können. Somit werden im BMLV zum Schutz nationaler klassifizierter Informationen, Kryptogeräte verwendet, die wahrscheinlich oder bekannterweise unter der Mitwirkung ausländischer Nachrichtendienste entwickelt wurden. Andere Länder vergleichbarer Größe (z.B.: Niederlande, Schweiz) setzen auf nationale Lösungen.

Daher soll eine Lösung entworfen werden, wo ein NCA (Nationaler Crypto Algorithmus) verwendet und implementiert wird, inklusive nationaler, programmierbarer Hardwarekomponenten. Somit wäre eine Chain of Trust, also eine Vertrauenskette von Hardware- und Softwarekomponenten von der Endentität bis zum Stammzertifikat validiert, möglich.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Sind die nötigen Technologien und das Know-how in Österreich verfügbar?
- Können Open Source Produkte verwendet werden?
- Welche Konfiguration und Anpassungsmöglichkeiten gibt es im Nachhinein?
- Welches geeignete Schlüsselmanagement kann eingesetzt werden oder muss ein eigenes entwickelt werden?
- Wo (bei welchen Komponenten/Bauteilen) endet eine Nationale Chain of Trust?
- Wäre eine Produktion im Hinblick auf die aktuelle Marktsituation wirtschaftliche machbar?
- Ist ein TEMPEST (Norm für die Abstrahlsicherheit) Upgrade wirtschaftlich und zweckmäßig?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.8 Die effiziente Behandlung digitaler Beweismitteln

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at , cc: andreas.bednarek@bmj.gv.at

Im Bereich der Strafverfolgung werden IT-ForensikerInnen bei der digitalen Beweismittelsicherung häufig mit zwei fundamentalen Problemstellungen konfrontiert. Zum einen muss der Wahrheitsgehalt aufgrund von Manipulationen innerhalb der Daten oftmals angezweifelt werden und zum anderen führte die rasante Entwicklung bei Speichermöglichkeiten in den letzten Jahrzehnten dazu, dass die vorhandenen Datenmengen explosionsartigen angestiegen sind und deren genutzte Speicherorte zentral auf Endgeräten und lokalen Servern wie auch dezentral in sogenannten Cloud-Diensten liegen können.

Datenmanipulation tritt heutzutage in Form von einfachen Fälschungen der Metadaten (z.B. Zeitstempelmanipulation) bis hin zu komplexen KI gestützten, sogenannten Deepfakes, in Erscheinung. Sie kann aber auch durch eine Unschärfe bei der Beweismittelsichtung bzw. -analyse angewandten Methode entstehen. Als Beispiel kann hier die Texterkennung von optischen Medien (Optical Character Recognition, OCR) erwähnt werden.

Die Problematik mit den enormen Mengen an Daten wiederum hat dazu geführt, dass vollständige Sicherungen von Datenbeständen aufgrund der komplexen Speicherstrukturen, die in den meisten Fällen völlig ortsunabhängig sind, de facto nicht mehr durchführbar sind.

Beide Problemstellungen müssen proportional in engem Zusammenhang gesehen werden, da maschinengestützte Methoden bei der Datenauswertung aufgrund der Datenmenge und strukturellen Komplexität als absolut unerlässlich anzusehen sind und damit jedoch auch gleichzeitig die Wahrscheinlichkeit eine ungewollte Datenmanipulation in Gang zu setzten steigt. Eine vollinhaltliche manuelle Vorgehensweise bei Methoden sowie bei der Gesamtsichtung aller Daten um den tatsächlichen Wahrheitsgehalt dieser festzustellen, ist wiederum wegen des verfahrensbeschleunigenden Ansatzes mit der Pflicht zur objektiven Wahrheitserforschung sowie aber auch einer angemessenen Verfahrensdauer aufgrund der Datenqualität und wegen der in den meisten Fällen nicht vollständigen Datensicherung (aufgrund der Menge) unmöglich.

Um die Datenqualität wie z.B. die Erkennung von Deepfakes zu heben, existieren bereits Ansätze zur maschinengestützten Verifikation. Flexible, erweiterbare Systeme, welche eine breite Unterstützung für die Plausibilisierung von Daten ermöglichen und gleichzeitig die Anforderungen für den Einsatz im forensischen und analytischen Strafrechtsbereich erfüllen, fehlen jedoch noch.

Ergänzend zur Verifikation von Daten ist in gewissen Bereichen auch deren Korrektur vorstellbar. Als Beispiel sei hier eine Bitcoin-Adresse angeführt, welche durch Texterkennung (OCR) aus einem optischen Medium extrahiert wurde. Da eine Bitcoin-Adresse klar definierten Kriterien unterliegt, ist neben der Erkennung und der Verifikation auch eine Korrektur maschinengestützt automatisch denkbar. Für die auf diesen Ergebnissen aufbauenden Ermittlungen muss allerdings zu jeder Zeit ersichtlich sein, wie und aus welchem Grund entsprechende Daten korrigiert wurden, da sonst die bereits zuvor erwähnten forensischen Anforderungen im Strafrechtsbereich nicht erfüllt werden.

Abseits einer rein automatischen Datenverifikation samt Korrektur ist eine manuelle jedoch maschinengestützte Verifikation und Korrektur in bestimmten Szenarien, wo rein automatische Methoden nicht ausreichend erscheinen, sinnvoll. Hier können bei semantischen Inhalten die aktuellen Fortschritte im Bereich der künstlichen Intelligenz, insbesondere von Large Language Models, für eine Verifikation und Korrektur unterstützende Informationen liefern.

Bei maschinengestützten Methoden (insbesondere bei KI-Algorithmen) ist aufgrund der Unschärfe der Resultate eine manuelle Kontrolle sowie eine Qualitätssicherung jedoch unerlässlich.

Zukünftige Lösungen müssen das Aufgreifen, Korrigieren, Hinzufügen, Erweitern, Integrieren, Fusionieren, etc. der Resultate von automatischen als auch manuellen Ergebnissen ermöglichen. Eine optimale Ergänzung der menschlichen kognitiven Fähigkeiten mit maschinellen Analysemethoden sollte angestrebt werden, um die Stärken beider Welten zu nützen.

Um wiederrum die große Menge an Beweismittelrohdaten in einer möglichst frühen Verfahrensphase filtern und priorisieren zu können, ist es notwendig relevante und nicht relevante Daten möglichst automatisch und maschinengestützt zu kategorisieren. Forensische Analysesoftwarelösungen bieten auch hier bereits gewisse Filtermöglichkeiten an. Hierfür muss der Datenbestand aber meist aufwendig aufbereitet und analysiert werden.

Der technologische Fortschritt in der maschinengestützten Analyse von Daten hat sich aufgrund der Einführung von KI-Methoden stark verbessert. Für gezielt eingesetzte Anwendungen (zum Beispiel in der Text- und Multimedia-Analyse) liefern KI-Algorithmen gute Ergebnisse, welche für maschinelle Unterstützungsleistungen bei der Filterung und Priorisierung von Beweismittelrohdaten genutzt werden können.

Eine technisch-inhaltliche Methode, welche als vorgelagerter Schritt automatisch bei jedem Fall zur Anwendung gelangt wäre hier insbesondere iSd Verfahrensbeschleunigung des § 9 StPO dienlich.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung des Forschungsstandes zur automatischen, maschinengestützten Relevanzprüfung, Filterung und Priorisierung von Daten im digital-forensischen Bereich, maschinengestützten Verifikation und Korrektur von Daten
- Erarbeitung eines Konzeptes zur Relevanzprüfung, Filterung und Priorisierung von Beweismittelrohdaten, Implementierung eines Werkzeuges zur Qualitätssicherung, manueller Kontrolle der maschinellen Ergebnisse und zur Verifikation und Korrektur von Beweismitteldaten
- Evaluierung von Schnittstellen forensischer Softwarelösungen für die weitere Aufbereitung und Analyse dieser Daten unter Betrachtung der gewonnenen Relevanzen und Priorisierungen und zur Interoperabilität in Bezug auf Verifikations- und Korrekturdaten
- Entwicklung und Implementierung eines flexiblen und erweiterbaren Softwareframeworks zur Relevanzprüfung, Filterung und Priorisierung von Beweismittelrohdaten sowie Verifikation und Korrektur von Beweismitteldaten (unter Berücksichtigung des entsprechenden Konzeptes sowie der Schnittstellen der forensischen Softwarelösungen)
- Evaluierung von KI-Methoden zur Filterung und Priorisierung von Multimediadaten
- Evaluierung von maschinengestützten Methoden auf semantischen Dateninhalten zur Filterung und Priorisierung
- Evaluierung von maschinengestützten Technologien (insbesondere KI) zur Detektion und Kennzeichnung von Daten mit höchstpersönlichem (in der Regel nicht verfahrensrelevanten) Inhalt (z.B. Gesundheitsdaten, sexuelle Orientierung, ...) sowie zur manuellen Verifikations- und Korrekturunterstützung
- Evaluierung von multimodalen Methoden zur Kategorisierung von Beweismittelrohdaten

- Implementierung von entsprechend positiv evaluierten Methoden/Technologien im angeführten Softwareframework
- Erhebung der für die Strafverfolgung relevanten Szenarien in denen eine Verifikation des Wahrheitsgehalts und eine mögliche Korrektur von Beweismitteldaten entscheidend ist.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.9 Prison Intelligence als Mittel zur Erhöhung der dynamischen Sicherheit in Justizanstalten

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at , cc: andreas.bednarek@bmj.gv.at

Das Konzept der dynamischen Sicherheit in Justizanstalten stellt die Beziehung zwischen den Mitarbeitern in Justizanstalten und den Insass:innen in den Mittelpunkt der Betrachtung. Deren Optimierung kann einen wichtigen Beitrag zur Sicherheit in Justizanstalten bieten. Essentiell dafür ist es, die Insass:innen zu kennen und aus den vorhandenen Informationen Erkenntnisse über mögliche problematische Situationen und Konstellationen ableiten zu können – Prison Intelligence leistet also einen wichtigen Beitrag zur dynamischen Sicherheit in Justizanstalten.

Im österreichischen Strafvollzug werden die Daten der Insass:innen in digitaler Form strukturiert in verschiedenen Anwendungen gespeichert. Teilweise liegen Insassen-Informationen allerdings auch in der Form von elektronischen Dokumenten sowie im Papierform vor. In ihrer Gesamtheit stellen diese Daten einen großen Wissensschatz dar, der sich aber aufgrund von nicht verknüpften Datensilos und fehlender Analysemöglichkeiten nur schwer materialisieren lässt. Natürlich ermöglichen die vorhandenen Anwendungen die Konsumation von zuvor erfassten Informationen zu Insass:innen, und über Business Intelligence Werkzeuge werden Entscheidungsträgern aggregierte Informationen zur Verfügung gestellt. Zur Beantwortung spezieller Fragestellungen betreffend Insass:innen und Insass:innen - Gruppen sind die Verantwortlichen allerdings auf die Unterstützung von IT- Experten angewiesen.

Im Rahmen dieses sicherheitspolitischen Forschungsschwerpunktes soll untersucht werden, wie dieser Datenschatz gehoben werden kann, ohne die Verantwortlichen im Strafvollzug zu IT-Experten ausbilden zu müssen. So sollen zum Beispiel niederschwellige Ansätze wie Chat Bots untersucht werden, mit deren Hilfe die Justizwachebeamten die als Wissensmodell vorliegenden Informationen über Insass:innen in natürlicher Sprache befragen können. Auch alternative Ansätze zur Visualisierung von vorhandenem Wissen und zur Navigation in bestehenden Daten können einen wertvollen Beitrag zum Thema Prison Intelligence bieten. Ebenso wäre es denkbar zu erforschen, wie die vorhandene Datenbasis mittels Methoden der künstlichen Intelligenz untersucht werden könnten, um daraus neue Schlüsse zu

ziehen. Auf dieser Basis könnte ein System selbständig auf Missstände und verdächtigte Konstellationen hinweisen.

Folgender Forschungsbedarf ergibt sich aus diesem Zusammenhang:

- Forschung, wie die vorhandenen Daten des österreichischen Strafvollzugs einer Analyse im Sinne von Prison Intelligence besser zugänglich gemacht werden können
- Erforschung, wie die optimale Interaktion mit den vorhandenen Daten aussehen könnte und wie entsprechende User Interfaces aussehen würden, um diese bestmöglich zu unterstützen. Insbesondere eine Prüfung, ob natürlich-sprachige Kommunikation mit einer Wissensdatenbank auch auf komplexe Fragestellungen verlässliche Antworten liefern kann und die Erforschung wie interessante Datenkonstellationen visualisiert werden können, um eine optimale Navigation in den Daten zu ermöglichen
- Erforschung von Methoden, wie die Benutzer solcher Systeme einfach (und auch für technische Laien verständlich) in die Lage versetzt werden können, die vom System ermittelten Antworten zu validieren - im Falle von natürlich-sprachig kommunizierten Fragestellungen auch betreffend die korrekte Interpretation der Fragestellungen. Ist im Entscheidungsprozesse eine künstliche Intelligenz eingebunden, sollen Methoden erforscht werden, wie deren Erkenntnisse im Sinne einer explainable AI (XAI)transparent gemacht werden können
- Forschung, ob Methoden der künstlichen Intelligenz sinnvoll eingesetzt werden können, um mit der nötigen Verlässlichkeit automatisiert interessante Datenkonstellationen zu finden
- Prüfung, inwieweit die beforschten Themen in Hinblick auf den AI ACT der europäischen Union zu bewerten sind
- Sozialwissenschaftliche Forschung über Akzeptanz und Vertrauenswürdigkeit solcher Lösungen seitens der Justizwachebeamten.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.10 Sichere technologieunterstützte (Re-)Integration

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at, cc: andreas.bednarek@bmj.gv.at

Der österreichische Strafvollzug ist ein moderner Betreuungsvollzug, der die Menschenrechte und die (Re-)Integration der Insass:innen ins Zentrum stellt. Vor diesem Hintergrund gewinnen die Digitalisierung des Alltags der Insass:innen sowie die Möglichkeiten der Insass:innen zur digitalen Kommunikation und zur Konsumation von digitalen Inhalten immer mehr an Bedeutung. Diese für Insass:innen neuen Technologien ermöglichen ihnen Selbstständigkeit, bereiten für ein Leben in der Gesellschaft vor und minimieren Rückfälligkeit. Durch digitale Inklusion profitieren Insass:innen von einem erhöhten Selbstwertgefühl, welches ungewolltes Verhalten in der Haftanstalt minimiert und dadurch eine sichere Atmosphäre erzeugt. Dynamic Security (dynamische Sicherheit) zielt darauf ab, eine Umgebung zu schaffen, in der Insass:innen aktiv in ihre (Re-)Integration einbezogen werden.

Die soziologischen Hintergründe werden aktuell im Zuge des KIRAS F&E-Dienstleistungsprojekts „DigitRes“ untersucht. Im Umfeld einer Justizanstalt müssen Angebote wie Internetnutzung, Videotelefonie oder Email aber immer auch mit den Sicherheitserfordernissen und dem Abschließungsgrundsatz in Einklang gebracht werden, weshalb in der Praxis entsprechende Kontrollen vorzusehen sein werden. Es ist zu befürchten, dass eine künftige großflächige Nutzung digitaler Angebote durch Insass:innen durch personell nicht leistbare Kontrollaufwände verhindert werden könnte. Vor diesem Hintergrund soll geprüft werden, ob eine teilweise oder vollständige Automatisierung dieser Prüfungen mittels künstlicher Intelligenz ermöglicht werden kann.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung, ob durch künstliche Intelligenz oder andere geeignete Methoden eine Inhaltsanalyse und Bewertung von besuchten Webseiten in Echtzeit erfolgen kann. Prüfung, ob auf Basis eines solchen Systems auch der Inhalt auf sich potentiell rasch ändernde und durch die breite Öffentlichkeit anpassbare Inhalte wie die Wikipedia für Insassen freigegeben werden könnte
- Untersuchung der Machbarkeit, ob eine künstliche Intelligenz in der Lage wäre, die Nutzung von Kommunikationsmöglichkeiten auf Webseiten (wie Foren oder Chats) zuverlässig in Echtzeit zu erkennen und zu blockieren
- Forschung, wie die Inhalte asynchroner (und potentiell fremdsprachlicher) schriftlicher Kommunikation auf schädliche und gefährliche Inhalte geprüft werden können
- Forschung, ob und wie die Inhalte synchroner, audiovisueller (und potentiell fremdsprachlicher) Kommunikation in Echtzeit auf schädliche und gefährliche Inhalte geprüft werden können
- Prüfung der Verlässlichkeit solcher Methoden
- Forschung, wie die Entscheidungsprozesse einer künstlichen Intelligenz für Laien im Sinne einer explainable AI (XAI)transparent gemacht werden können.
- Erforschung alternativer Technologien, welche eine Resozialisierung unterstützen könnten (z.B. Virtual Reality)
- Prüfung, inwieweit die beforschten Themen in Hinblick auf den AI ACT der europäischen Union zu bewerten sind
- Sozialwissenschaftliche Forschung in Hinblick auf die Akzeptanz der Insassen für automatisierte Kontrollen im Vergleich zur herkömmlichen Überwachung durch Justizwachebeamte.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.11 Mixed Reality-unterstütztes Training für die Vorbereitung auf Einsätze in Krisensituationen

Kontakt: Bundesministerium für europäische und internationalen Angelegenheiten, Mag. Philipp Agathonos (BMEIA)
E-Mail: Philipp.agathonos@bmeia.gv.at

Die Stärkung des zivilen und militärischen Krisenmanagements ist ein Kernbereich der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der EU und eine Priorität des Strategischen Kompasses für Sicherheit und Verteidigung. Um sicherheitspolitische Herausforderungen hinsichtlich Friedenssicherung, und Stärkung der internationalen Sicherheit effizient zu bewältigen, bedarf es entsprechend qualifizierten Personals. Zivile und militärische Fachkräfte (inkl. EU, UNO, OSZE Personal, NGOs, …) die in Krisengebieten entsendet werden, müssen bestimmte Skills für internationale Kriseneinsätze im Vorfeld erlernen. Ausbildungsstätten führen Ausbildungen im Rahmen von europäischen Trainingsnetzwerken wie dem European Security and Defence College (ESDC) durch. Die Trainingscurricula umfassen neben Theorieeinheiten auch Simulationen, in denen Trainer:innen und Trainingsassistent:innen (Schauspieler) bestimmte Rollen (z.B. Flüchtling, Grenzbeamte) übernehmen. Hierbei wird Outdoor beispielsweise auf Feld- und Waldwegen in größeren Regionen (mehrere Kilometer) trainiert. Die Möglichkeiten von Simulationsübungen sind einerseits begrenzt durch Personalressourcen (z.B. Anzahl an Schauspielern), und andererseits durch limitierte Möglichkeiten, das gesamte Spektrum von Aspekten (z.B. gesprengte Brücken, Klimakatastrophen, Vielzahl verletzter Personen) überzeugend darzustellen. Mixed Reality (MR) Technologien bieten hier neue Möglichkeiten, um das Training durch virtuelle Darstellung zusätzlicher Dimensionen (z.B. Gefahren, Klimaaspekte, Flüchtlingsdörfer) zu ergänzen und damit das Training überzeugender zu gestalten. Dies ermöglicht ein vielfältigeres und damit realistischeres Trainieren von abgeleiteten Entscheidungsfindungen (z.B. Umgang mit Gefahrenräumen) in großflächigen simulierten Krisengebieten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation notwendiger Skills (Wegfindung, Verhandlung) bei Kriseneinsätzen, die mittels MR- Technologien überzeugenderer trainiert werden können als in bisherigen Simulationsübungen
- Identifikation von Dimensionen / Faktoren, die via MR im Training miteingebracht werden sollen
- Erarbeitung eines MR-Trainingsframeworks welches es ermöglicht im Outdoor-Trainingsgelände, das sich über mehrere Kilometer erstrecken kann, zusätzliche Komplexitätsebenen einzubauen (z.B. Einblenden von Flüchtlingen, Zeltlagern, Klimakatastrophen, etc.)
- Bereitstellung von Technologien, die eine Kombination aus Schauspielern und virtuell eingeblendeten Trainingselementen ermöglichen. So können sich die Trainierenden wie bisher in der Simulation bewegen und interagieren, jedoch durch die MR zusätzliche Faktoren in der Entscheidungsfindung und im Handeln miteinbeziehen

- Outdoor-Tracking von Trainierenden um im Trainingsszenario mit den virtuellen Elementen sowie den anderen Trainierenden interagieren zu können
- Möglichkeiten für Trainer:innen, in die Simulation steuernd einzugreifen
- Evaluierung von Möglichkeiten, die obengenannte Technologie in derzeitige Ausbildungsprogramme zu integrieren.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.12 Effizientere und zielgerichtetere Kontrollen im Internet für einen verbesserten Verbraucher:innenschutz entlang der Lebensmittelkette – Forschung im Bereich Mystery Shopping und Web-Crawler-Entwicklung für Zwecke der Betrugsprävention und Marktüberwachung

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: carolin.krejci@gesundheitsministerium.gv.at

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)
E-Mail: karin.rainer@ages.at

Österreichische Verbraucher:innen kaufen zunehmend Lebensmittel und andere Waren des täglichen Bedarfs im Internet. Das einhergehende Risiko, dass Bürger:innen beim Online-Shopping auf betrügerische Angebote sowie gesundheitsgefährdende Produkte stoßen, wächst durch den über Ländergrenzen weltweiten Internethandel. Prävention und eine effektive amtliche Kontrolle sind entscheidend im Kampf gegen Cybercrime, um die Schäden bei Bürger:innen so gering wie möglich zu halten. Je schneller und umfassender potenziell gefährliche Produkte sowie Internetfallen erkannt werden, desto effektiver kann davor gewarnt und können entsprechende amtliche Gegenmaßnahmen ergriffen werden.

Die zuständigen Behörden müssen zur zielgerichteten und effizienten Überwachung des gesamten „Marktplatzes Internet“ sowie zur Sicherstellung der Nahrungsmittelversorgung als kritische Infrastruktur neue und effiziente Kontrollinstrumente- und -mechanismen etablieren. Dabei gibt es bereits Instrumente, die weiter ausgebaut werden können und sollen (z.B. Crawler und Know-how zur Betrugsprävention bei der Watchlist Internet, KI-Einsatz beim Fake-Shop Detector etc.).

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

Verwendung von spezialisierten und bedarfsgerechten Web Crawlern:

- Prävention und eine effektive amtliche Kontrolle sind entscheidend im Kampf gegen Cybercrime, um die Schäden bei Bürger:innen so gering wie möglich zu halten. Je schneller und umfassender potenziell gefährliche Produkte sowie Internetfallen erkannt werden, desto effektiver kann davor gewarnt und können entsprechende amtliche Gegenmaßnahmen ergriffen werden

- Das gezielte Auffinden von Betrugsfallen sowie potenziell gesundheitsschädlichen Produkten ist aufgrund der Menge an im Internet verfügbaren Seiten bzw. Anbietern auch durch verstärkten Personaleinsatz nicht mehr möglich. Effektive Abhilfe schafft nur die Entwicklung von spezialisierten Crawlern, wie z.B. für die Identifikation von Fake-Shop-Clustern, gefährlichen Produkten, betrügerischen Werbeanzeigen (Google, Instagram, etc.) sowie für das automatisierte Auslesen von Anbieterdaten und weiteren Anwendungen.

Entwicklung der Möglichkeit einer anonymen und verdeckten Probenbeschaffung im Internet

- Die effektive amtliche Kontrolle ist entscheidend um Schäden bei Bürger:innen so gering wie möglich zu halten. Je schneller und umfassender potenziell gefährliche Produkte erkannt werden, desto effektiver kann vor Produkten gewarnt und Produktrückrufe als amtliche Gegenmaßnahme ergriffen werden. Die Möglichkeit für die Behörden eine anonyme und verdeckte Probenbeschaffung („mystery shopping“) stellt ein ganz wesentliches zentrales zukünftiges Kontrollinstrument dar. Bei dieser Methode bezieht die Behörde inkognito als vermeintliche/r Verbraucher:in die Ware über den Webshop des Unternehmens der Lebensmittel- und Konsumgüterbranche
- Die bisher verwendeten Methoden zur (anonymen) Probenbeschaffung stellen lediglich Provisorien dar, die sich durch Auslagerung der Transparenz und Qualitätssicherung entziehen, oder die jederzeit unbrauchbar werden können (z.B. durch Änderung von Geschäftsbedingungen von privaten Dienstleistern). Sie erfordern außerdem den Einsatz von persönlichen Daten und Zahlungsmitteln von öffentlichen Bediensteten, die dadurch großen Risiken ausgesetzt werden.

Langfristige Risikoreduktion und Vernetzung

- Im Rahmen des Projektes soll durch eine intensive Vernetzung mit inländischen und ausländischen Einrichtungen ein Austausch von Best Practice Beispielen stattfinden, um so einen Beitrag zur Verbesserung der Resilienz im Risikomanagement auf nationaler und europäischer Ebene zu leisten.

Für Österreich ist der jetzige Zeitpunkt für die Entwicklung einer wirkungsvollen Internetkontrolle besonders durch die aktuelle Weltlage relevant, da es durch die Verknappung mancher Stoffe am Markt zu Engpässen sowie auch Veränderungen bei den Rezepturen und daher zu massiven Auswirkungen in der Lebensmittelkette kommen kann (wie auch Global Food Regulatory Science Society im Vergleich mit der Krise im Jahr 2007 warnt).

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.13 Sichere Sekundärnutzung von Gesundheitsdaten für resiliente Gesundheitssysteme

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
E-Mail: : Robert.Scharinger@gesundheitsministerium.gv.at

Kontakt: Gesundheit Österreich GmbH (GÖG)
E-Mail: alexander.degelsegger-marquez@goeg.at

Gesundheitskrisen stellen eine große Herausforderung für die Gesundheitsversorgung, aber auch für die Steuerung von Gesundheitssystemen dar. So sind je nach Bedrohungslage bestimmte Datenerhebungen, -verknüpfungen und -verarbeitungen Voraussetzung für zielgerichtete Analysen, deren Ergebnisse erst die Handlungsfähigkeit der sicherheitspolitischen und Public Health-Akteure sicherstellen. Im Anlassfall müssen die richtigen Daten zur richtigen Zeit in ausreichender Qualität zur Verfügung stehen. Technischen Infrastrukturen und Prozesse müssen skalierbar sein und eine effiziente Datenverarbeitung erlauben.

Im Covid-19 Variantenmanagementplan der Bundesregierung ist beispielsweise die Problematik der Fragmentierung der österreichischen Gesundheitsdatenlandschaft angesprochen.

Es wird auf die Wichtigkeit der Nutzung der Möglichkeiten der Digitalisierung hingewiesen, etwa in Bezug auf automatisierte Schnittstellen bei der Befüllung von Public Health-Registern. Besonderes Augenmerk wird auf die Verantwortlichkeit der Bundesebene für das Krisenmanagement gelegt. In der Ausgestaltung der Governance-Strukturen für Gesundheitsdaten spielen nicht zuletzt deshalb die Bundesakteure eine zentrale Rolle.

Auf europäischer Ebene bieten die Entwicklungen rund um den Europäischen Gesundheitsdatenraum (European Health Data Space, EHDS) Möglichkeiten die Sekundärnutzung von Gesundheitsdaten für sicherheitspolitische und Public Health-Zwecke weiterzuentwickeln.

Fazit:

- Die Sekundärnutzung von Gesundheitsdaten wird wichtiger und umfassender (vgl EHDS)
- es gilt diese auf eine sichere Weise zu ermöglichen (Angriffsvektoren durch technische und organisatorische Maßnahmen minimieren, Sicherheitsrisiken überwachen, etc.)
- effektive und sichere Gesundheitsdaten-Sekundärnutzung macht Gesundheitssysteme resilienter (raschere und präzisere Reaktion auf Systemschocks etc.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie kann und soll eine Dateninfrastruktur des Bundes gestaltet sein, die unter Wahrung von Datenschutz- und Datensicherheitsstandards ein effizientes und effektives Management von Gesundheitskrisen ermöglicht?
- Welche Prozesse braucht es für Datenerhebung, -auswertung und Governance (Entscheidungsfindung, Stakeholder-Einbindung, etc.)? Wie können diese so konzipiert werden, dass sie ressourcenschonend aufrechterhalten und im Anlassfall skaliert, werden können?
- Wie lassen sich die durch den EHDS veränderten rechtlichen Rahmenbedingungen in Österreich nutzen, um resiliente Dateninfrastrukturen und Prozesse zur Erhebung und Auswertung krisenrelevanter Gesundheitsdaten aufzubauen?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.14 Cybersicherheit für Fahrzeuge

Kontakt: ÖAMTC
E-Mail: daniel.deimel@oeamtc.at

Kontakt: BMK
E-Mail: andreas.herndler@bmk.gv.at/ krima@bmk.gv.at

Die zunehmende Verbreitung automatisierter Fahrfunktionen in modernen Fahrzeugen, der Bedarf an mehr Konnektivität sowie die Fortschritte beim autonomen Fahren führen zu einer raschen Digitalisierung von automobilen Systemen. Damit einhergehend steigt auch die Anzahl der in einem Fahrzeug eingesetzten Software-Komponenten, womit die Angriffsfläche bezüglich Cybersicherheit wesentlich erhöht wird. Besonders kritisch sind die Ausnutzung möglicher Angriffsmöglichkeiten für Organisationen (z.B. Einsatzorganisationen), die Fahrzeugflotten mit einer großen Anzahl von Fahrzeugen des gleichen Typs einsetzen, da mit demselben Angriff potentiell die Funktion vieler Fahrzeuge gestört werden kann. Folglich müssen Sicherheitssysteme von automobilen Systemen auf dem neuesten Stand gehalten werden und auch gegen aktuelle Cyber-Bedrohungen geschützt sein.

Die potentielle Vielfalt an neuen Bedrohungen und Schwachstellen in Kombination mit der Komplexität und Heterogenität automobiler Systeme erfordern jedoch automatisierte Ansätze für das Monitoring der Bedrohungen, und das Testen von Angriffsvektoren an verschiedensten Systemkonfigurationen. Trotz der dringenden Notwendigkeit, den gesamten Prozess von der Entdeckung neuer Ausnutzungsszenarien bis hin zum Testen zu unterstützen und zu automatisieren, gibt es keine industrietauglichen, automatisierten und durchgängigen Ansätze.

Ziel ist die Erhöhung der Cybersicherheit im Automobilbereich, indem eine umfassende, strukturierte und automatisierte Sicherheitsanalyse und -prüfung ermöglicht wird. Dabei stellt die hohe Komplexität automobiler Systeme und die

anfänglich unklaren Black-Box-Bedingungen ein nicht triviales Problem dar. Bei der Entwicklung einer automatisierten Lösung sind folgende Themenbereiche zu berücksichtigen:

- Die frühzeitige Identifikation von Sicherheitsbedrohungen und Schwachstellen, unter Nutzung einer Vielzahl von Quellen, wobei es notwendig ist, proaktiv nach solchen Informationen zu suchen und sie zu sammeln, bevor sie in Angriffsdatenbanken verfügbar werden, um möglichen Angriffen einen Schritt voraus zu sein
- Die Identifizierung kritischer Komponenten in komplexen, automobilen Systemen sowie deren Eigenschaften und Funktionen
- Die Erstellung geeigneter Testfälle für die identifizierten Komponenten, unter Nutzung der Informationen über potentielle Sicherheitsbedrohungen und Schwachstellen.

Weitere Ziele sind:

- Unterstützung des Kompetenzaufbaus der teilnehmenden Akteure hinsichtlich Cybersicherheit von Fahrzeugen
- Demonstration einer Lösung zur Einschätzung des Gefährdungspotentials eines Fuhrparks.

Es soll die Grundlage für eine industrietaugliche Lösung geschaffen werden, die eine automatisierte, vergleichbare, wiederholbare und effiziente Art der Prüfung der Cybersicherheit von automobilen Systemen ermöglicht. Die Ergebnisse sollen in vielerlei Hinsicht von Nutzen sein, von der formalen Überprüfung von erfassten Systemmodellen (im Hinblick auf seine Vollständigkeit) bis hin zur einfachen Erstellung von Dokumentationen der erzielten Ergebnisse. Es sollen (wieder-)verwendbare Daten generiert werden, um eine Cybersicherheitsanalyse und anschließend Penetrationstests für eine Vielzahl verschiedener automobiler Systeme durchführen zu können.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.15 Bekämpfung von Desinformation durch die Analyse und Detektion von Fake-News-Netzwerken

Kontakt: Bundesministerium für Landesverteidigung (BMLV)
E-Mail: sicherheitsforschung@bmlv.gv.at

Im Rahmen Hybrider Konflikte stellen Fake-News-Netzwerke eine erhebliche Bedrohung für die Demokratie und die Gesellschaft dar. Diese Netzwerke verbreiten absichtlich falsche Informationen, um Meinungen zu manipulieren, politische Agenden voranzutreiben und das Vertrauen in Medien und Institutionen zu untergraben. Neue Technologien wie die rasante Entwicklung von generativer künstlicher Intelligenz (KI) haben die Art und Weise, wie Fake-News-Netzwerke Bots in der Kommunikation einsetzen, revolutioniert. Generative KI hat die Fähigkeiten

von Bots erheblich verbessert und ermöglicht die weitgehende Automatisierung menschenähnlicher Interaktionen.

Die Auswirkungen von Desinformations-Kampagnen haben durch den Einsatz dieser Technologien eine neue Dimension und Bandbreite erreicht. Fake-News Netzwerke können dabei Einfluss auf politische Entscheidungsträger oder Wahlen nehmen, die Gesellschaft polarisieren, das Vertrauen der Öffentlichkeit in die demokratischen Institutionen erschüttern oder wirtschaftlichen Schaden anrichten.

Um diesen Bedrohungsbildern zu begegnen, ist es notwendig, die Komplexität dieser Netzwerke zu verstehen und geeignete Gegenmaßnahmen zu entwickeln. Damit soll einerseits das Verständnis für Hybride Konflikte und somit ein Beitrag zur Stärkung und Sicherung der demokratischen Institutionen geleistet werden. Andererseits soll ein besseres Verständnis von Fake-News-Netzwerken dazu beitragen, die Mechanismen hinter der Erstellung und Verbreitung von gefälschten Inhalten zu entschlüsseln und mögliche Schwachstellen zu identifizieren.

Die zu entwicklenden Demonstratorsysteme sollen einer flexiblen und skalierbaren Architektur folgen, um die einfache Integration in vorhandene Systeme zu ermöglichen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwicklung von Detektionsalgorithmen sowie eines Demonstratorsystems zur Identifikation und Analyse von Fake-News-Netzwerken, die Bots und automatisierte Systeme zur Verbreitung von Desinformation nutzen
- Entwicklung von Abwehrmechanismen gegen Fake-News-Netzwerke, um die Ausbreitung von Desinformation einzudämmen
- Analyse der von Fake-News Netzwerken ausgehenden Gefahren für die Demokratie sowie deren Auswirkungen auf Wahlen, politische Entscheidungsträger, Wirtschaft etc.
- Entwicklung von Tools und Know-How zur Identifikation und Eindämmung von Fake-News als Beitrag zur Stärkung und Sicherung der demokratischen Institutionen
- Entwicklung eines Demonstratorsystems zur Simulation von generativer KI bzw. Bots in Fake-News Netzwerken zur Identifikation von möglichen Schwachstellen und Gegenmaßnahmen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.16 Cybersicherheit allgemein

Hier können weiterhin alle kooperativen Projekte eingereicht werden, welche das Thema Cybersicherheit treffen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.4 K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für F&E-Dienstleistungen

3.4.1 Definition von Anforderungen für QKD-Lösungen für das Zentrale Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau

Kontakt: Bundeskanzleramt, ABTEILUNG I/8: CYBERSICHERHEIT, GOVCERT, NIS BÜRO UND ZAS (BKA)
E-Mail: cybersicherheit@bka.gv.at

Quantentechnologie ist seit einigen Jahren ein stark beforschtes Thema, das als sogenannte disruptive Innovation Potentiale und Bedrohungen gleichermaßen beinhaltet.

Die EU-Strategie für Cybersicherheit aus dem Jahr 2020 identifiziert neben Quantencomputing insbesondere Quantenverschlüsselung als Schlüsseltechnologie, um die Resilienz, Souveränität und Führungsrolle der EU, die Sicherstellung eines Kapazitätenaufbaus zur Vorbeugung und Reaktion auf Cyberbedrohungen sowie die Unterstützung eines globalen und offenen Cyberraumes in und durch die EU zu erreichen. Die EU unterstützt Quantenforschung mit einem Budget von mindestens einer Milliarde Euro durch das sogenannte Quantum Flagship.

Im Bereich Quantenverschlüsselung stellt sich Österreich die Frage, wie sich die Verwaltung bestmöglich auf zukünftige Szenarien vorbereiten kann und bestehende Strukturen weiterhin sicher betreiben und weiterentwickeln kann.

Bei Quantenverschlüsselung geht es einerseits um die Frage, wie bestehende (nicht auf Quantenverschlüsselung basierende) kryptografische Systeme so gestaltet werden können, dass sie bestmöglich gegenüber konventionellen und zukünftigen Quanten-kryptografischen Analysemöglichkeiten (Post-Quanten-Kryptografie) geschützt sind. Andererseits geht es um die Frage, wie Systeme durch die neuen kryptografischen Lösungen selbst sicherer werden (Quanten Key Distribution). Für beide Szenarien müssen zukünftig Rahmenbedingungen in der österreichischen Verwaltung geschaffen werden, sodass bestehende Strukturen an diese Entwicklungen angepasst werden können.

Ein wichtiger Anwendungsanfall dabei ist die sichere Kommunikation über Glasfasernetze zwischen den Ministerien und dem Zentralen Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau. Das ZAS dient zur Sicherstellung der Durchführung wichtiger Verwaltungsaufgaben in Ausnahmesituationen sowie als behördliches Backupdatacenter und Langzeitarchivierungssystem. Die hierfür notwendige Datenstrecke zwischen dem Behördennetz in Wien und dem Ausweichsystem in St. Johann muss entsprechend gesichert werden. Die Absicherung der Kommunikation bedarf eines sicheren Schlüsselaustauschs.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Technische Prüfung und Realisierbarkeit einer QKD-Lösung zwischen dem Zentralen Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau und dem Wiener Behördennetz und Konzipierung einer prototypischen QKD-Lösung, die Rücksicht auf insbesondere die Schlüsselübertragung über weitere geografische Distanzen nimmt
- Identifizierung von rechtlichen und organisatorischen zu lösenden Fragen betreffend den möglichen Einsatz einer entsprechenden QKD-Lösung in diesem Behördenkontext unter Rücksichtnahme von europäischen Entwicklungen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.2 Fachkräftebedarf im Bereich der Cybersicherheit

Kontakt: Bundeskanzleramt (BKA)
E-Mail: ncc@bka.gv.at

Die Österreichische Strategie für Cybersicherheit (ÖSCS 2021) listet als eines ihrer Ziele: „Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Resilienz im Bereich Cybersicherheit zu erhöhen, die Nachfrage des Arbeitsmarktes zu erfüllen und die Cyberkriminalität nachhaltig zu bekämpfen“.

Mit der sich ständig weiterentwickelnden Cyber-Landschaft geht naturgemäß auch ein erhöhter Bedarf an Arbeitskräften in diesem Bereich einher, welcher derzeit nicht ausreichend gedeckt ist. Gemäß Angaben der Europäischen Kommission fehlten im Jahr 2022 zwischen 260.000 und 500.000 Cybersicherheitsexpert:innen in der Europäischen Union. Aus strategischer Sicht stellt dieser Fachkräftemangel einen kritischen Sicherheitsfaktor dar.

Für die erfolgreiche und effektive Umsetzung aktueller regulatorischer Vorhaben auf EU-Ebene - wie etwa der Cyber Resilience Act, der Cybersecurity Act, der Cyber Solidarity Act oder das geplante NIS-2-Gesetz - sind zahlreiche IT-Spezialist:innen sowohl für private als auch für öffentliche Einrichtungen nötig. In diesem Lichte ist es auch wichtig, Menschen mit verschiedenen Profilen anzusprechen und den Frauenanteil in diesen Branchen zu erhöhen, welcher derzeit EU-weit laut Schätzung der Europäischen Kommission bei nur rund 20% liegt.

Um dieser Nachfrage bestmöglich nachzukommen und entsprechende Vorgehensweisen zu treffen, ist ein detaillierter Gesamtüberblick über die aktuelle Lage des Expert:innenmangels im IT-Bereich notwendig.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung der Arbeitsmarktsituation im Bereich Cybersicherheit in Österreich
- (inkl. Erhebung, welche spezifischen Berufsprofile von IT-Expert:innen unter Berücksichtigung des European Cybersecurity Skills Framework (ECSF) in

Österreich benötigt werden; Erhebung der Diversität von Fachkräften (insbesondere Anteil von Frauen); Erstellung einer Liste des nationalen Ausbildungsangebots, inkl. Studiengänge und Fachausbildungen im Bereich der Cybersicherheit; Analyse des öffentlichen Bewusstseins in Bezug auf diese Bildungsmöglichkeiten bzw. auf Berufsmöglichkeiten im Cybersicherheitsbereich allgemein; Erhebung von öffentlichen und privaten Initiativen im Bereich Cybersecurity Skills)
- Entwicklung eines Konzepts zur Erhebung und Erhebung der Prognose des voraussichtlichen Bedarfs an Cybersicherheitsexpert:innen in den kommenden Jahren für Österreich
- Erarbeitung von Handlungsempfehlungen unter Berücksichtigung von möglichen zukünftigen Schwerpunkten für Förderprogramme sowie unter Berücksichtigung des Bedarfs von KMUs und der Steigerung des Frauenanteils/Diversität
- Mögliche Vorschläge für verbesserte internationale Zusammenarbeit
- Mögliche Identifizierung von weiterem Forschungs- und Erhebungsbedarf in diesem Bereich.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.3 Steigerung der Cybersicherheit und Resilienz landwirtschaftlicher Prozesse und Systeme zur Gewährleistung der Versorgungssicherheit Österreichs

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Sektion II – Landwirtschaft und ländliche Entwicklung (BML)
E-Mail: johann.doppelbauer@bml.gv.at

Die zunehmende Digitalisierung und Vernetzung hat in den letzten Jahren nicht nur Vorteile gebracht, sondern bringt für Unternehmen und Staaten auch ein Gefahrenpotential durch Angriffe aus dem Internet. Cyberangriffe auf Lebensmittel- und Landtechnikbetriebe (AGCO, John Deere, JBS, Salzburg Milch, …) führten in letzter zu großer Medienberichterstattung und Besorgnis. Aufgrund der aktuellen Entwicklungen ist zu erwarten, dass die Cyberangriffe auf die Landwirtschaft und den vor- und nachgelagerten Bereich zunehmen werden. V.a. der zunehmende Einsatz von vernetzten Geräten, das vielfach unzureichend vorhandene Bewusstsein der Bedrohungslage bei den Landwirt:innen und mangelhafte Sicherheitsmaßnahmen bieten weitere Angriffsmöglichkeiten. Aufgrund der Bedeutung der Versorgungssicherheit ist Handlungsbedarf vorhanden. Ziel ist es, den Landwirtschafts- und Lebensmittelsektor besser auf Cyberbedrohungen vorzubereiten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Untersuchung der Vulnerabilität der österreichischen Landwirtschaft und Risikobewertung
- Darstellung der Risikofaktoren und mögliche Gegenmaßnahmen im Sinne des „resilient smart farming“

- Analyse von landwirtschaftlichen Betrieben mit unterschiedlichen Voraussetzungen (Zugang zu digitalen Lösungen, infrastrukturelle Gegebenheiten, etc.)
- Abhängigkeiten und Angriffsmöglichkeiten im Zusammenhang mit digitalen Anwendungen in der Landwirtschaft und im vor- bzw. nachgelagerten Bereich.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.4 Entwicklung eines OpenSource-Frameworks (EUPL lizenziert) zu Murensimulationen mit Schwerpunkt auf österreichische Verhältnisse

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft, Abt. III/4 – Wildbach- und Lawinenverbauung und Schutzwaldpolitik, DI Andreas Pichler (BML)
E-Mail: andreas.pichler@bml.gv.at

Der Prozess „Murgang“ ist eine langsam bis schnell abfließende Suspension aus Wasser, Feststoffen und Wildholz, die sich dann entwickelt, wenn in kurzer Zeit große Geschiebemengen verfügbar werden. In einem alpin geprägten Land wie Österreich kommt dieser Prozesstyp sehr häufig vor, insbesondere in steilen Wildbacheinzugsgebieten. Der Prozessablauf von Murgängen ist insgesamt sehr komplex, was zusätzlich die Prognosefähigkeit (z.B. im Rahmen der Gefahrenzonenplanung) wie auch die generelle hydrologische und hydraulische Planung erschwert. Da die räumliche Ausbreitung bei großen und seltenen Ereignissen vor allem bei Murgängen nur schwer vorhersehbar ist, ist es notwendig, sich auch numerischer Modelle zu bedienen, um die Vorhersagesicherheit zu erhöhen.

In Österreich werden seitens der Wildbach- und Lawinenverbauung wie auch von Zivilingenieuren derzeit nur 2 numerische Simulationsmodelle für die Berechnung von Muren herangezogen – einerseits das amerikanische Modell „Flo-2D“ und andererseits das schweizer Modell „RAMMS“. Beide sind nicht auf typisch österreichische Bedingungen (aufgrund Geologie, Geotechnik, Hydrologie, Hydraulik, Rheologie etc.) abgestellt, wofür umfangreiche Kalibrierungen im Vorfeld der Simulationen notwendig sind.

Ziel wäre daher – ähnlich wie das kürzlich fertiggestellte „AvaFrame – Avalanche Simulation Framework“ für Schneelawinen - ein offenes Framework – im Hinblick auf die Programmierungsstruktur – für Murprozesse als Basis zu generieren. Mittels verschiedener Programmmodule werden österreich-spezifische Verbesserungen in den Simulationen sichergestellt. Das Framework soll so aufgestellt sein, dass es ebenso für die wissenschaftliche Entwicklung durch Forschungszentren und in der akademischen Ausbildung verwendet werden kann. Damit ist die Integration neuester Entwicklungen in den operationellen Betrieb der WLV bzw. Zivilingenieurbüros nach einer Testphase einfach möglich. Das neue Framework soll zur Unterstützung bei der Gefahrenzonenplanung, Sachverständigentätigkeit sowie Planung und Dimensionierung von Schutzmaßnahmen durch die WLV und anderer

Institutionen sowie in der Murenforschung dienen. Mittel- und langfristig soll auch das Wissen anderer Institutionen in Österreich (z.B. ÖBB, ASFINAG, Landesgeologie etc.) in das Projekt eingebunden und dadurch die Murenmodellierung auf eine breitere wissenschaftliche und ingenieurpraktische Basis gestellt werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Weiterentwicklung der Grundlagenanalyse zu physikalischen Grundgrößen der Prozessinitiierung, -entfaltung, -ablauf, -wirkung
- Standardisierung (mind. auf ÖNORM-Basis)
- Implementierung dieser standardisierten Größen in ein 3D-Rechenmodell (OpenSource), segmentiert in: Inputmodule, Berechnungsmodule, Analysemodule, Darstellungsmodule und Protokollmodule inkl. der Integration der Wirkung von Schutzinfrastruktur auf den Prozess „Murgang".

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.5 Data Science und KI für Trendanalysen von Mediendaten in seltenen Sprachen

Kontakt: Bundesministerium für europäische und internationalen Angelegenheiten, Mag. Philipp Agathonos (BMEIA)
E-Mail: Philipp.agathonos@bmeia.gv.at

Für GSVP-Missionen in Osteuropa und im Raum Kaukasus sind Anwendungen moderner Medienanalyse-Tools nicht nutzbar, da der Stand der Technik nur durch die wichtigen Hauptsprachen gedeckt ist, Textanalysen in seltenen Sprachen wie Armenisch, Aserbaidschanisch oder Georgisch aber nicht durchgeführt werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse des Einsatzes modernster KI-Trainingsmethoden wie „AI-Transfer Learning" und kostengünstige Erstellung von qualitativ hochwertigen Trainingsdaten für moderne Data Science und KI-basierte Textanalysen in seltenen Sprachen im osteuropäischen und kaukasischen Raum
- Es soll untersucht werden, ob durch spezielle KI-Trainingsmethoden eine aufwändige Erstellung von Trainingsdaten in seltenen Sprachen ersetzt werden kann. Dies würde zu einer massiven Kostensenkung für die Entwicklung von Analysemodule beitragen und ermöglichen, KI-Textanalysen auch für seltene Sprachen einsetzen zu können
- Ein vortrainiertes Sprachmodell (z.B. BERT - Bidirectional Encoder Representations from Transformers) oder ein „Basismodell", das mit einer ressourcenreichen Sprache wie Englisch trainiert wurde, soll verwendet werden, um ein Modell für seltenere Sprachen zu „optimieren". Zuerst müssen Daten in der seltenen Sprache gesammelt und von Experten kommentiert werden. Dann kann das Basismodell auf diesen Datensatz fein abgestimmt werden, sodass es

sich an die linguistischen Merkmale dieser spezifischen Sprache anpassen kann. Dieses fein abgestimmte Modell kann dann als Ausgangspunkt für weitere Trainings oder nachgelagerte Anwendungen in der seltenen Sprache verwendet werden und stellt eine entscheidende Ressource für zusätzliche Aufgaben der Verarbeitung natürlicher Sprache wie die Erkennung von Sexismus oder Extremismus dar.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.6 Cybersecurity-Literacy – Wissensvermittlung in der oberen Sekundarstufe in Österreich

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF)
E-Mail: AL Mag. Eduard Staudecker, MBA, Eduard.Staudecker@bmbwf.gv.at

Die Digitalisierung ist wesentliche Voraussetzung für die Entwicklung einer modernen Gesellschaft. Zur Vorbereitung und Bewusstseinsbildung im Umgang mit digitalen Werkzeugen und zum Verhalten im digitalen Raum muss Cybersicherheit in der schulischen Bildung berücksichtigt werden, um ein resilientes Ökosystem für Cybersecurity bilden zu können. In Ergänzung des „Themenbereichs Bildung" der Österreichische Strategie für Cybersicherheit 2021 soll eine Studie die Rahmenbedingungen für die Integration von Cybersecurity-Aspekten in den Schulunterricht strukturiert analysieren und mögliche pädagogische Ansätze zur Wissensvermittlung erarbeiten. Schwerpunkt der Ausarbeitung sollen Themenbereiche und Wissensgebiete sein, die im Besonderen für 14- bis 19-Jährige Schülerinnen und Schüler im österreichischen Bildungssystem (d.h. Berufsschulen, AHS, BMHS) anschlussfähig sind. Insbesondere sollen Inhalte mit Arbeitsmarktbezug, die die Beschäftigungsfähigkeit der genannten Zielgruppe erhöhen ein zentraler Aspekt der Studie sein. Lehrkräfte sollen von den pädagogischen Instrumenten, Sachanalysen und Unterrichtsmaterialien profitieren.

Zielsetzung ist somit eine wissenschaftlich fundierte Aufbereitung des Themas zum Nutzen des BMBWF, um in gezielten Bereichen des Schulsystems für dieses Thema zu sensibilisieren und berufs- und arbeitsmarktbezogene Aspekte zu den aktuell laufenden Überlegungen zur Lehrplanentwicklung beizusteuern.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwicklung eines bildungspolitischen, gesellschaftlichen und sozio-technischen Ansatzes zur Vermittlung des Themenbereichs Cybersecurity für 14- bis 19-Jährige mit besonderem Bezug zum beruflichen Kompetenzerwerb und zum Arbeitsmarkt
- Definition und wissenschaftliche Darstellung bedarfsorientierter spezifischer Cybersecurity-Themenbereiche und Wissensgebiete (mit Bezug zur Zielgruppen, dem Arbeitsmarkt und konkreten Berufen) auch im Hinblick auf Unterrichtsmaterialien und Schulbücher

- Ausarbeitung wissenschaftlicher Grundlagen möglicher Wissensvermittlungsstrategien und zeitgemäßer didaktischer Konzepte samt konkreten Empfehlungen für die Unterrichtsgestaltung
- Beantwortung der Frage, wie Jugendliche auf die Herausforderungen der Cybersecurity im digitalen Raum vorbereitet werden können
- Ausarbeitung der Frage, wie bewusstseinsbildende Maßnahmen gestaltet werden können bzw. wie am Thema Haltung und Einstellung im Unterricht gearbeitet werden kann?
- Rückmeldungen zur Anschlussfähigkeit des Themas in bestehenden Unterrichtsfächern (z.B. digitale Grundbildung, Informatik) und Ausbildungsbereichen (z.B. HTL Informatik, digBiz HAK)
- Berücksichtigung von genderrelevanten, sozioökonomischen und kulturellen Bedarfen bei den Ausarbeitungen
- Schaffung eines Überblicks über die wesentlichen Akteure an der Schnittstelle Cybersecurity und Schule in der oberen Sekundarstufe in Österreich.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.7 Instrumente zur Bewertung der rechtlichen, technischen und ethischen Einsatzmöglichkeiten von KI-gestützten Technologien in eJustice Anwendungen

Kontakt: Bundesministerium für Justiz (BMJ)
E-Mail: sicherheit@bmj.gv.at, cc: andreas.bednarek@bmj.gv.at

Der Einsatz von Künstlicher Intelligenz (KI) im Bereich der Rechtspflege und Strafverfolgung ist von zunehmender Bedeutung.

So wird beispielsweise im Rahmen der Initiative „Justiz 3.0“ die Akten- und Verfahrensführung an den österreichischen Gerichten und Staatsanwaltschaften sukzessive digitalisiert, wodurch sich auch neue Einsatzbereiche zur Verarbeitung, Analyse und Auswertung dieser Informationen ergeben.

Andere potenzielle Anwendungs- und Entwicklungsfelder liegen z.B. im Management des Strafvollzugs, der kriminalistischen Analyse großer und/oder komplexer Datensätze oder der Bewertung der Verlässlichkeit von Beweismitteln.

KI-basierter Anwendungen im Bereich der Rechtspflege und Strafverfolgung bergen jedoch erhebliche Risiken, sowohl in sicherheitstechnischer Hinsicht als auch im Hinblick auf die subjektiven Rechte der von solchen Systemen und Entscheidungen betroffenen Personen.

In Ergänzung zu den bestehenden grundrechtlichen Vorgaben und datenschutzrechtlichen Regelwerken wird auf europäischer Ebene auf diese Entwicklungen mit einer Vielzahl von Maßnahmen und Rechtsakten reagiert (Digitalisierungsstrategie), die für den Einsatz KI-basierter Anwendungen zu beachten sind (siehe z.B. den Entwurf der „Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz“ (COM/2021/206 final), die

„Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law“ oder die „European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment“ usw.). Zudem werden diverse sektorale Verordnungen aktualisiert, um KI-bedingte Risiken mitzuberücksichtigen.

Bei der Entwicklung und Anwendung KI-basierter Technologien sind daher künftig eine Vielzahl an sich teils ergänzenden, überschneidenden oder ausschließenden rechtlichen sowie ethischen Anforderungen zu prüfen und technische Voraussetzungen zur Gewährleistung der Cybersicherheit zu erfüllen.

Aus Sicht der Bedarfsträger ist dabei besonderes Augenmerk auf das Prinzip der Rechtsstaatlichkeit (Legalitätsprinzip) zu legen, welches bereits im Zuge der Konzeption bzw Entwicklung der Technologie entsprechend beachtet werden sollte (Rule of Law by Design).

Gerade im Kontext von innovativen Forschungsprojekten kann es auch zu technischen Entwicklungen kommen, welche letztlich aufgrund der gegebenen Rechts- und Risikolage nicht für den Einsatz im Justizalltag geeignet sein könnten.

Um finanzielle und personelle Ressourcen zweckmäßig zu investieren, sind etwaige Risiken soweit möglich bereits im Vorfeld abzuklären.

Weiters gilt es für verantwortliche Stellen bei tatsächlicher Anwendung einer KI-basierter Technologien verschiedene Transparenz-, Dokumentations- und Nachweispflichten umzusetzen sowie frühzeitig eine Reihe von Grundsätzen und Prinzipien in technischer und organisatorischer Form zu implementieren (siehe Data Governance sowie die Konzepte Privacy by Design, Privacy-Preserving Machine Learning sowie Privacy-enhancing Technologies).

Von zunehmender Bedeutung ist für Anwender in diesem Zusammenhang auch die verantwortliche Durchführung von Risiko,- Technik-, Datenschutz- oder Menschenrechts-Folgenabschätzungen (Impact Assessments).

In der Mitigierung etwaiger Risiken und unerwünschter Folgen für die Rechte und Freiheiten der Betroffenen geht es dabei nicht zuletzt auch um das Ergreifen von Maßnahmen und Verfahren zur Gewährleistung der Genauigkeit, Robustheit und Sicherheit derartiger Systeme.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Forschung und Analyse zu technischen, rechtlichen sowie organisatorischen Voraussetzung für die Entwicklung und Integration neuer eJustice-Anwendungen für die bestehende IT-Landschaft
- Entwicklung eines Prüfschemas, einer Anleitung bzw. eines Instruments zur Gewährleistung der Compliance (in den Bereichen Grund- und Menschenrechte, Rechtstaatlichkeit, Datenschutzrecht, sowie Cybersicherheit) für jede neue Entwicklung oder Integration KI-basierter Anwendungen im Bereich der Rechtspflege und Strafverfolgung („Compliance-Toolkit“)

- Interdisziplinäre Analyse und systematischer Vergleich der verschiedenen normativen und methodischen Vorgaben zur Durchführung bzw. Umsetzung von Folgenabschätzungen und Risikoanalysen für neue Hochrisiko-Technologien im Bereich der Rechtspflege und Strafverfolgung
- Interdisziplinäre Entwicklung eines Instruments bzw. Schemas zur praktisch-operativen Durchführung von Folgenabschätzungen und Risikoanalysen für Hochrisiko-Technologien im Bereich der Rechtspflege und Strafverfolgung („Impact-Assessment-Toolkit“)
- Entwicklung einer digitalen Anwendung oder Nachweis der technischen Machbarkeit (Proof of Concept) für eine digitale Anwendung zur Unterstützung bei der Einhaltung der verschiedenen Vorgaben zur Grundrechte-, Datenschutz-, Cybersicherheits- und Rechtsstaatlichkeits-Compliance im Rahmen der Prozesse einer typischen KIRAS Antragstellung unter Berücksichtigung der Möglichkeiten im FFG eCall System (Kooperative F&E Projekte).

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.8 Cybersicherheit allgemein

Hier können weiterhin alle F&E-Dienstleistungen eingereicht werden, welche das Thema Cybersicherheit treffen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.5 KIRAS/K-PASS F&E-Dienstleistung Innovation AKUT

Die KIRAS/K-PASS-KMU-Initiative Innovation AKUT ist eine neue Möglichkeit zur Umsetzung von sicherheitsrelevanten Projekten in einem sehr hohen Umsetzungslevel; erwartet werden Einreichungen im Bereich TRL 6-8, sofern es sich nicht um Zertifizierungsmaßnahmen handelt. Ziel der zu erbringenden F&E-Dienstleistungen ist die Generierung neuen Wissens im öffentlichen Interesse unter Anwendung wissenschaftlicher Methoden. Insbesondere soll durch diese Initiative die zumindest probehafte Einführung von neuen Techniken, Methoden oder Produkten beim beteiligten Bedarfsträger lanciert werden.

F&E-Dienstleistungen (F&E-DL) sind definiert durch die Erfüllung eines Ausschreibungsinhaltes in einem bestimmten Zeitraum. Die Leistungserbringung erfolgt durch F&E-Tätigkeiten. Die Leistung steht im öffentlichen Interesse und ist in geteilten Rechten durch den Auftragnehmer und durch den Auftraggeber zu verwerten. Allgemein gelten Dienstleistungen als F&E-DL, wenn sie darauf ausgerichtet sind, neue Erkenntnisse zu gewinnen, ab TRL 6 – 7 in Ausnahmefällen TRL 8, sofern es sich nicht nur um Zertifizierungsmaßnahmen handelt.

Antragstellern steht es frei, während der ersten Ausschreibungsphase vom 30.10.2023 bis 31.01.2024 (danach eventuell weitere Ausschreibungsphasen bis zum Verbrauch des für diese Initiative vorgesehenen Budgets bzw. spätestens 30. Oktober 2024) Projektanträge einzureichen, welche einen sicherheitspolitischen Nutzen aufweisen müssen und die unter diesem Punkt (Kapitel 3.5) genannten Voraussetzungen erfüllen.

Verwendet wird das FFG-Instrument „C17 F&E-Dienstleistung“ mit folgenden Einschränkungen:

- Maximale Vertragssumme 100.000.- inkl. ev. UST. Eine höhere Einreichung führt daher zu einer Formalablehnung
- Laufzeit max. 12 Monate, eine Verlängerung der Laufzeit kann in begründeten Ausnahmefällen gewährt werden
- Konsortialvorschrift: Die BIEGE/ARGE muss aus mindestens einem österreichischen KMU und mindestens einem Bedarfsträger bestehen
- Ausländische Partner sind nicht teilnahmeberechtigt
- Finanzierungsart: Finanzierungsquote 100 %.

1 Mio. EUR wird für diese Initiative zur Verfügung stehen. Besondere Anforderungen: Es gelten die Grundprinzipien der Transparenz, der Gleichbehandlung, des Diskriminierungsverbotes und des freien und lauteren Wettbewerbes. Auftraggeber und Auftragnehmer haben an den Projektergebnissen jeweils nicht ausschließliche Nutzungs- und Verwertungsrechte.

Die Ausschreibungsschwerpunkte sind im Kapitel 3.2 (für KIRAS. Schutz kritischer Infrastruktur) und Kapitel 3.4 (für K-PASS. Cybersicherheit) angeführt.

Es können alle F&E-Dienstleistungen eingereicht werden, welche die Themen Schutz kritischer Infrastruktur allgemein und Cybersicherheit allgemein treffen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

4 INSTRUMENTE UND ANFORDERUNGEN

4.1 Kooperatives F&E-Projekt

Beachten Sie den Leitfaden für Kooperative F&E-Projekte (v4.3).

4.1.1 Konsortien

Konsortien für kooperative F&E-Projekte müssen aus mindestens zwei Partnern bestehen. Die Anzahl der Projektteilnehmer ist nach oben formal nicht begrenzt.

Über diese standardisierte Auflage hinausgehend müssen sich bei allen kooperativen F&E-Projekten im Rahmen von KIRAS/K-PASS:

- mindestens ein Bedarfsträger aus dem öffentlichen oder privaten Bereich als Konsortialteilnehmer
- mit mindestens einem Partner aus der Wissenschaft (universitäre oder außeruniversitäre Forschungseinrichtung) als Konsortialteilnehmer und
- einem Partner aus der Wirtschaft als Konsortialteilnehmer sowie
- einem Vertreter der Geistes-, Sozial- und Kulturwissenschaften (GSK) als Konsortialteilnehmer oder Subauftragnehmer des Konsortiums.

zusammenschließen (mindestens 1+1+1(+1) Partner).

Um ein ausgewogenes Kooperationsverhältnis zu gewährleisten muss:

- die Kostensumme aller F&E-Partner unter 70 % liegen
- die Kostensumme aller Wirtschaftspartner unter 70 % liegen.

Der Einbindung von Bedarfsträgern und GSK-Vertretern kommt eine besondere Rolle zu.

Für das Konsortium kann nur ein Projektpartner (Unternehmen, Forschungseinrichtung) mit Standort in Österreich gegenüber der FFG als Konsortialführer auftreten.

Die Ausschreibung wendet sich inhaltlich auch an Organisationen des Bundes. Mit dem Bund idente Bedarfsträger können zwar als Projektpartner einreichen, jedoch erhalten keine Förderung.

Im Falle eines Konsortiums ist eine Einreichung eines ausländischen Partners und Förderung bis maximal 10 % der angesuchten Gesamtfördersumme des Projekts möglich.

Die Grenze für Drittkosten liegt bei 20 % der Gesamtkosten je Partner. Liegen sie darüber, muss die Überschreitung in der Projektbeschreibung begründet werden. Insgesamt dürfen die Drittkosten 20 % der Gesamtprojektkosten nicht überschreiten.

Bei kooperativen F&E-Projekten muss beachtet werden, dass verpflichtend ein Beratungsgespräch bei einer öffentlichen Wirtschaftsförderungsagentur im Projektverlauf eingeplant werden muss, um die wirtschaftliche Verwertung von Ergebnissen zu unterstützen.

4.1.2 Forschungskategorien

Forschungs- und Entwicklungsprojekte können als kooperative Projekte eingereicht werden. Von der Projektart sind Industrielle Forschung und Experimentelle Entwicklung mit unterschiedlichen Maximalfördersätzen vorgesehen.

Details zu den Forschungskategorien, sowie Fragen die eine Einstufung in die Projektkategorie erleichtern, finden Sie in dem Leitfaden für Kooperative F&E-Projekte (v4.3).

4.2 F&E-Dienstleistung

Beachten Sie den Leitfaden für Forschungs- und Entwicklungsdienstleistungen (v4.4).

4.2.1 Allgemein

Es werden Studien und studienähnliche Vorhaben im Rahmen des aktuellen Schwerpunktes finanziert. Zielgruppe sind Nutzer im weiteren Sinne. Die beauftragten Maßnahmen können eigenständige Vorhaben darstellen oder in direktem Zusammenhang mit anderen Projekten aus KIRAS stehen.

Aufgrund der Breite des Themas können grundsätzlich all jene Studien bzw. studienähnlichen Vorhaben beauftragt werden, die dazu beitragen, das Gemeinwesen in Österreich sicherer und stabiler zu gestalten (z.B. Studien zur Perzeption von Sicherheit und Sicherheitstechnologien, Machbarkeitsstudien, etc.). Diese Maßnahmen können auch einen Beitrag dazu leisten, dass oben genannter umfassender Sicherheitsbegriff in Berücksichtigung der KIRAS/K-PASS Ziele weiterentwickelt und für Teilbereiche näher definiert wird.

Zu den speziellen Anforderungen des F&E-Dienstleistungsfokus Innovation AKUT siehe Kapitel 3.5.

4.2.2 Bietergemeinschaften

Das Instrument richtet sich an Partner aus den Bereichen Wirtschaft und Wissenschaft sowie an Bedarfsträger. Für eine BIEGE/ARGE kann nur ein Unternehmen oder Forschungseinrichtung mit Standort in Österreich gegenüber der FFG als Einzelbieter bzw. BIEGE/ARGE- Leiter auftreten.

Die Ausschreibung wendet sich inhaltlich auch an Organisationen des Bundes. Mit dem Bund idente Bedarfsträger können zwar nicht als BIEGE/ARGE- Leiter auftreten, sind jedoch ermutigt sich an der Ausschreibung zu beteiligen.

Im Falle eine BIEGE/ARGE können ausländische Partner teilnehmen, allerdings dürfen diese nicht mehr als 10 % der Finanzierung bekommen.

Die Grenze für Drittkosten liegt bei 20 % der Gesamtkosten je Partner. Liegen sie darüber, muss die Überschreitung in der Projektbeschreibung begründet werden. Insgesamt dürfen die Drittkosten 20 % der Gesamtprojektkosten des Projekts nicht überschreiten.

4.2.3 Auflagen und Bedingungen durch Jury

Im Rahmen des Bewertungsverfahrens für „Forschungs- und Entwicklungsdienstleistungen“ können von der Jury zusätzliche Auflagen unter den im folgenden Abschnitt angeführten Rahmenbedingungen definiert werden, welche in weiterer Folge Vertragsbestandteil werden. Hierbei handelt es sich um eine abschließende Aufstellung aller durch die Jury gegebenenfalls dem einzelnen Bieter/der einzelnen Bieterin vorzuschreibenden Auflagen und Bedingungen.

Das Anbot muss eine detaillierte Personalkostenplanung sowie ausreichende Belege (Lebensläufe) für den Nachweis der korrekten Einstufung aller am Projekt beteiligten Personen beinhalten. Während des Begutachtungsprozesses können die Personalkosten um bis zu 50 % gekürzt werden, wenn:

- Der für die F&E-Dienstleistung beantragte Personalaufwand in seiner Höhe im Anbot nicht detailliert und nachvollziehbar begründet wurde oder
- die Angemessenheit der Kosten nicht gegeben ist (z.B. der Inhalt eines Lebenslaufs die für das Projekt getätigte Einstufung der Funktion des entsprechenden Mitarbeiters nicht ausreichend belegt).

Bei für das Projekt vorgesehener Reisetätigkeit muss das Anbot eine detaillierte Reiseplanung sowie eine realistische Reisekostenschätzung (Preis) beinhalten. Der Jury ist es vorbehalten, die beantragten Reisetätigkeiten gesamt oder nur in Teilen anzuerkennen. Während des Begutachtungsprozesses können die Reisekosten um bis zu 50 % gekürzt werden, wenn:

- der Aufwand an Reisetätigkeit im Anbot nicht detailliert und nachvollziehbar begründet wurde, oder
- die Angemessenheit der Kosten nicht gegeben ist.

Arbeitspakete können ganz oder zum Teil gestrichen werden. Die Projektgesamtkosten sind in diesem Fall anteilsmäßig zu reduzieren. Ein überarbeiteter Kostenplan ist in diesem Fall vom Bieter/der Bieterin im eCall der FFG vorzulegen. Arbeitspakete oder Teile davon können durch die Jury gemäß den nachfolgenden Parametern gekürzt werden, wenn:

- eine angebotene Leistung enthalten ist, welche für die Zielerreichung des Projekts nicht notwendig erscheint oder
- eine angebotene Leistung, welche bereits durch ein nationales bzw. EU-Projekt hinreichend abgedeckt ist.

4.2.4 Weitere Anforderungen und Vorgaben zur Einreichung von F&E-Dienstleistungen

Folgende Nachweise sind als Anhang im eCall hochgeladen:

- Auszug aus dem Gewerberegister oder beglaubigte Abschrift des Berufsregisters oder des Firmenbuches (Handelsregister) des Herkunftslandes des:der Bietenden oder die dort vorgesehene Bescheinigung oder – falls im Herkunftsland keine Nachweismöglichkeit besteht – eine eidesstattliche Erklärung des Bewerbers, jeweils nicht älter als 12 Monate
- Bietende, die im Gebiet einer anderen Vertragspartei des EWR-Abkommens oder in der Schweiz ansässig sind und die für die Ausübung einer Tätigkeit in Österreich eine behördliche Entscheidung betreffend ihre Berufsqualifikation einholen müssen, haben ein darauf gerichtetes Verfahren möglichst umgehend, jedenfalls aber vor Ablauf der Angebotsfrist einzuleiten. Gleiches gilt für Subunternehmende, an die der:die Bietende Leistungen vergeben will. Der:die Bietende hat den Nachweis seiner:ihrer Befugnis durch die Vorlage der entsprechenden Gewerbeberechtigung grundsätzlich in seinem:ihrem Angebot zu führen. Die Auftraggeberin behält sich vor, die Befugnis von allfälligen Subunternehmern gesondert zu prüfen
- Aktueller Firmenbuchauszug (max. 6 Monate alt)
- Der:die Bietende hat auch einen Nachweis über den Gesamtumsatz und die Umsatzentwicklung für die letzten drei Jahre bzw. für den seit Unternehmensgründung bestehenden Zeitraum bei Newcomer:innen (darunter sind Unternehmen zu verstehen, die vor weniger als drei Jahren gegründet wurden) vorzulegen.

5 AUSSCHREIBUNGSDOKUMENTE

Reichen Sie das Projekt ausschließlich elektronisch via eCall ein.

Die Einreichung beinhaltet folgende **online** Elemente, die im eCall unter folgenden Menüpunkten zu erfassen sind:

- **Inhaltliche Beschreibung** umfasst die Darstellung der Projektinhalte
- **Arbeitsplan** beinhaltet die Darstellung der Arbeitspakete und Elemente des Projektmanagements wie Zeit-Managementplan (GANTT-Diagramm), Aufgaben, Meilensteine, Ergebnisse
- **Konsortium** beschreibt die Expertise der einzelnen Konsortiumsmitglieder
- **Kosten und Finanzierung** beschreibt alle Kostenkategorien pro Konsortiumsmitglied. Die Summen je Arbeitspaket werden automatisch im online Arbeitsplan angezeigt
- Die Risikomatrix ist als Grundlage zur Beurteilung des Risikos und des Risikomanagements im Projekt als Anhang zum inhaltlichen Antrag im eCall hochzuladen
- Als Teil des elektronischen Antrags können etwaige Anhänge (wie bspw. LOIs) nach wie vor über die eCall Upload-Funktion hochgeladen werden
- Sämtliche relevante Dokumente für die Ausschreibung finden Sie auf der Webseite der Ausschreibung.

Förderkonditionen, Ablauf der Einreichung und Förderkriterien sind im jeweiligen Instrumenten- bzw. Ausschreibungsleitfaden beschrieben. Die nachfolgende Übersicht zeigt für die jeweiligen Instrumente die relevanten Dokumente.

Das ist neu und vereinfacht: Bis dato erfolgte die Einreichung der gesamten Projektbeschreibung mit Hilfe einer Word-Vorlage. Anstelle einer Word-Vorlage setzt sich die Projektbeschreibung nun aus den folgenden online Funktionen zusammen:

- Online-Inhaltliche Beschreibung (eCall)
- Online-Konsortium (eCall)
- Online-Arbeitsplan (eCall
- Online-Kosten und Finanzierung (eCall).

Mit der online Eingabe können nun einzelne Kapitel von der Konsortialführung an Partner delegiert werden. Alle Partner haben in der online Eingabe Lese- und Kommentier-Rechte. Ein integriertes Kommentier- und Versionsmanagement unterstützt bei der Zusammenarbeit im Antragstellungsprozess.

Im neuen online Antrag gibt es eine Zeichenbeschränkung bei der Erstellung, sollte diese überschritten werden, ist der Abschluss des Einreichprozesses nicht garantiert.

Weitere Hinweise finden Sie im Tutorial und unter den FAQs.

Als Teil des elektronischen Antrags sind etwaige Anhänge über die eCall Upload-Funktion anzuschließen.

Für Einreichungen im gewählten Instrument (siehe Ausschreibungsübersicht) sind die jeweils spezifischen Vorlagen zu verwenden.

Förderkonditionen, Ablauf der Einreichung und Förderkriterien sind im jeweiligen Instrumentenleitfaden beschrieben. Die nachfolgende Übersicht zeigt für die jeweiligen Instrumente die relevanten Dokumente.

Sämtliche relevante Dokumente für die Ausschreibung finden Sie im Download Center.

Tabelle 3: Ausschreibungsdokumente

Förderungs-/Finanzierungsinstrument bzw. sonstige Information	Verfügbare Ausschreibungsdokumente
Kooperative F&E-Projekte	– Leitfaden für Kooperative F&E-Projekte (v4.3) Als Anhang zum inhaltlichen Antrag - Upload als PDF im eCall: – Risiko Management Tabelle – MOU für Kooperative F&E Projekte – Antrag auf Klassifizierung – Angaben zur Einordnung des Vorhabens – Angabe zu Arbeitsplätzen – Eidesstattliche Erklärung zum KMU-Status (bei Bedarf)
F&E-Dienstleistungen	– Leitfaden für Forschungs- und Entwicklungsdienstleistungen (v4.4) Als Anhang zum inhaltlichen Antrag - Upload als PDF im eCall: – Risiko Management Tabelle – MOU für F&E-Dienstleistungen – Antrag auf Klassifizierung – Angaben zur Einordnung des Vorhabens – Angabe zu Arbeitsplätzen
Allgemeine Regelungen zu Kosten	– Kostenleitfaden (v3.0)

Hinweis: Die eidesstattliche Erklärung zum KMU-Status ist für unternehmerisch tätige Vereine, Einzelunternehmen und ausländische Unternehmen notwendig. In der zur Verfügung gestellten Vorlage muss – sofern möglich – eine Einstufung der letzten 3 Jahre lt. KMU-Definition vorgenommen werden

6 FÖRDERUNGS-/FINANZIERUNGSENTSCHEIDUNG UND RECHTSGRUNDLAGEN

Das Bundeministerium für Finanzen (BMF) trifft die **Förderungs- bzw. Finanzierungsentscheidung** auf Basis der Förderungs- bzw. Finanzierungsempfehlung des Bewertungsgremiums.

Die Ausschreibung basiert auf der Sonderrichtlinie KIRAS und Sonderrichtlinie K-PASS für die Österreichische Forschungsförderungsgesellschaft mbH zur Förderung von Sicherheitsforschung.

Bezüglich der Unternehmensgröße ist die jeweils geltende KMU-Definition gemäß EU-Wettbewerbsrecht ausschlaggebend. Hilfestellung zur Einstufung finden sie auf der KMU-Seite der FFG.

Sämtliche EU-Vorschriften sind in der jeweils geltenden Fassung anzuwenden.

Als **Rechtsgrundlage für „Forschungs- und Entwicklungsdienstleistungen“** wird der Ausnahmetatbestand § 9 Z 12 Bundesvergabegesetz 2018 angewendet.

7 WEITERE INFORMATIONEN

In diesem Abschnitt finden Sie Informationen über weitere Förderungsmöglichkeiten und Services, die im Zusammenhang mit Förderungsansuchen bzw. geförderten Projekten für Sie hilfreich sein können.

7.1 Hinweise zum Kostenplan

Informationen und Ausfüllhilfen:

- Kostenleitfaden (Version 3.0)
- eCall Tutorial

Der Konsortialführung obliegt das Projektmanagement sowie die Kommunikation mit der Förderungsstelle und den Projektpartner:innen. Dazu gehören die Prüfung der Kostenpläne aller Partner:innen im Hinblick auf Projektrelevanz, genehmigungskonforme Kostenhöhe, genehmigungskonforme Projektentwicklung und vorgabengetreue (Förderungsrichtlinien, Leitfaden) Förderungsansuchen der Partner:innen anhand der – von den Partner:innen bekannt gegebenen – Daten und Angaben. Beim Feststellen von Mängeln (lt. Checkliste) bei den Förderungsansuchen der Partner:innen sind diese im Kostenplan vom/von der jeweilige/n Partner:in zu korrigieren und die korrekte Version der Konsortialführung zu übermitteln.

7.2 Service FFG Projektdatenbank

Die FFG bietet als Service die Veröffentlichung von kurzen Informationen zu geförderten Projekten und eine Übersicht der Projektbeteiligten in einer öffentlich zugänglichen FFG Projektdatenbank an. Somit können Sie Ihr Projekt und Ihre Projektpartner besser für die interessierte Öffentlichkeit positionieren. Darüber hinaus kann die Datenbank zur Suche nach Kooperationspartnern genutzt werden.

Nach positiver Förderungsentscheidung werden die Antragstellenden im eCall System über die Möglichkeit der Veröffentlichung von kurzen definierten Informationen zu ihrem Projekt in der FFG Projektdatenbank informiert. Eine Veröffentlichung erfolgt ausschließlich nach aktiver Zustimmung im eCall System.

Nähere Informationen finden Sie auf der FFG-Seite zur Projektdatenbank.

7.3 Open Access Publikationen

Die Sichtbarkeit und Verfügbarkeit von Projektergebnissen hat sich in Programmen des BMF bereits bestens bewährt. Auch die Europäische Kommission setzt mit ihrer Empfehlung (2012/417/EU) zu Open Access auf den verbesserten Zugang zu wissenschaftlichen Publikationen, um eine wissens- und innovationsgestützte Wirtschaft zu erleichtern.

Daher sollen Projektergebnisse des Programms über geeignete Plattformen wie die KIRAS-Portal oder eine Projektdatenbank der FFG publiziert und frei zugänglich gemacht werden. Bei dieser Ausschreibung werden die geförderten Projekte und deren Ergebnisse (z.B. in Form publizierbarer Kurzfassungen) auf den oben erwähnten Plattformen der Öffentlichkeit zur Verfügung gestellt. Davon ausgenommen sind vertrauliche Inhalte (z. B. Projekte mit Patentanmeldungen, anderen Schutzstrategien wie Geheimhaltung, oder personenbezogene Daten). Um die Projektergebnisse übersichtlich und verständlich aufzubereiten, werden Hinweise für die Berichtslegung zu Projekten, die im Rahmen von KIRAS gefördert und durchgeführt werden, sowie korrespondierende Veranstaltungen mit entsprechenden Vorgaben zum Berichtswesen geregelt.

Die mit öffentlicher Förderung erzielten Forschungsergebnisse sind einer bestmöglichen Verwertung für Wissenschaft, Wirtschaft und Gesellschaft zuzuführen. In diesem Sinne ist bei referierten Publikationen, die mit Unterstützung der durch die FFG vergebenen Förderung entstehen, Open Access soweit wie möglich anzustreben. Als Prinzip gilt „as open as possible, as closed as necessary“, wie es auch für die Europäischen Förderungen angeführt wird.

Publikationskosten zählen zu den förderbaren Projektkosten.

7.4 Umgang mit Projektdaten – Datenmanagementplan

Ein Datenmanagementplan (DMP) ist ein Managementtool, das dabei unterstützt, effizient und systematisch mit in den Projekten generierten Daten umzugehen.

Für die Erstellung des DMP kann z.B. das kostenlose Tool DMP Online verwendet werden. Auch die Europäische Kommission bietet über ihre „Guidelines on FAIR Data Management“ Hilfestellung an.

Ein Datenmanagement-Plan beschreibt,

- welche Daten im Projekt gesammelt, erarbeitet oder generiert werden
- wie mit diesen Daten im Projekt umgegangen wird
- welche Methoden und Standards dabei angewendet werden
- wie die Daten langfristig gesichert und gepflegt werden und
- ob es geplant ist, Datensätze Dritten zugänglich zu machen und ihnen die Nachnutzung der Daten zu ermöglichen (sogenannter „Open Access zu Forschungsdaten“).

Es ist sinnvoll, Forschungsdaten, die referierten Publikationen zugrunde liegen und deren Veröffentlichung zur Reproduzierbarkeit und Überprüfbarkeit der publizierten Ergebnisse notwendig ist, offen verfügbar zu machen.

Werden Daten veröffentlicht, sollen die Grundsätze „auffindbar, zugänglich, interoperabel und wiederverwertbar“ berücksichtigt werden. Für eine optimale Auffindbarkeit empfiehlt es sich, die Daten in etablierten und international anerkannten Repositorien zu speichern (siehe auch die re3data Webseite).

7.5 Weitere Förderungsmöglichkeiten der FFG

Sie interessieren sich für andere Förderungsmöglichkeiten der FFG?

Das **Förderservice** ist die zentrale Anlaufstelle für Ihre Anfragen zu den Förderungen und Beratungsangeboten der FFG. Kontaktieren Sie uns, wir beraten Sie gerne!

Kontakt: FFG-Förderservice, T: +43 (0) 57755-0, E: foerderservice@ffg.at

Web: **https://www.ffg.at/foerderservice**

Weitere Förderungsmöglichkeiten der FFG finden Sie weiters hier.

8 ANHANG: CHECKLISTE FÜR DIE ANTRAGSEINREICHUNG

Bei der Formalprüfung wird das Förderungsansuchen auf formale Richtigkeit und Vollständigkeit geprüft. Bitte beachten Sie: **Sind die Formalvoraussetzungen nicht erfüllt und handelt es sich um nicht-behebbare Mängel, wird das Förderungsansuchen bei der Formalprüfung aufgrund der erforderlichen Gleichbehandlung aller Förderungs- bzw. Finanzierungsansuchen ausnahmslos aus dem weiteren Verfahren ausgeschieden und formal abgelehnt.**

Tabelle 4: Formalprüfungscheckliste

Kriterium	Prüfinhalt	Mangel behebbar	Konsequenz
Die Projektbeschreibung ist ausreichend befüllt vorhanden und es wurde die richtige Sprache verwendet.	Die Online-Projektbeschreibung ist vollständig auszufüllen. Sprache: Deutsch	Nein	Ablehnung aus formalen Gründen
Die verpflichtenden Anhänge gem. Ausschreibung liegen vor. [behebbar]	Zum Beispiel: Interessensbekundungen, Absichtserklärungen (Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Ja	Korrektur per eCall nach Einreichung
Der/Die Förderungswerbende ist berechtigt, einen Antrag einzureichen.	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Bei Konsortien: Die Projektbeteiligten sind teilnahmeberechtigt.	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Mindestanforderungen an das Konsortium	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Projektlaufzeit	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Höhe der Förderung	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen